

ROMANIAN MILITARY THINKING



ERIH PLUS EUROPEAN REFERENCE INDEX FOR THE HUMANITIES AND SOCIAL SCIENCES
INDEX COPERNICUS INTERNATIONAL
DOAJ
Central and Eastern European Online Library
MIAR Matriz de Información para el Análisis de Revistas
EBSCO
ROAD DIRECTORY OF OPEN ACCESS SCHOLARLY RESOURCES

ROMANIAN MILITARY THINKING

INTERNATIONAL SCIENTIFIC CONFERENCE

PROCEEDINGS



SECURITY STUDIES AND MILITARY SCIENCE INTERNATIONAL CONFERENCE,
ORGANISED BY THE DEFENCE STAFF

NOVEMBER 2024
BUCHAREST

6TH EDITION

PUBLISHER
THE DEFENCE STAFF

ORGANISING COMMITTEE

Chairman:
Lieutenant General Dragoș-Dumitru IACOB

Vice-Chairmans:
Lieutenant General Iulian BERDILĂ
Major General Valentin BRÎNZEI

Members:
Major General Remus-Hadrian BONDOR
Major General Liviu-Marian MAZILU
Major General Valerică VRĂJESCU
Major General Eugen MAVRIȘ, PhD
Brigadier General Professor
Ghiță BÂRSAN, BEng, PhD
Air Flotilla General
Assoc.Prof. Marius ȘERBESZKI, PhD

Secretariat:
Colonel Mircea BARAC
Alina PAPOI
Iulia SINGER
Diana Cristiana LUPU

DTP
Adelaida-Mihaela DANDEȘ

EDITORIAL OFFICE
București, str. Izvor nr. 110, sector 5
Postal code: 050564
Tel.: +4021.319.48.80/1005597; 1005596
Tel./fax: +4031.426.09.90
E-mail: gmr@mapn.ro
Web: gmr.mapn.ro

HIGH ROYAL DECREE NO. 3663 THROUGH WHICH "ROMÂNIA MILITARĂ" BECOMES THE OFFICIAL JOURNAL OF THE GREAT GENERAL STAFF

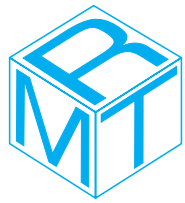


"Art. I – The official journal named "România Militară" is founded at the Great General Staff, starting 1 January 1898, in which all officers within the Armed Forces will find military studies. which interest their training.

Through the agency of this journal, all officers, belonging to all branches, who are in active duty, will be able to publish their personal papers and the ones that interest the Armed Forces".

Carol – King of Romania
Issued in Bucureşti on 8 December 1897

Printed
at Military Technical Publishing Centre
C __/____ B 1085/19.12.2024



ROMANIAN MILITARY THINKING
INTERNATIONAL SCIENTIFIC CONFERENCE PROCEEDINGS

DEFENCE AND MILITARY COOPERATION STRATEGIES FOR ENSURING SECURITY IN THE BLACK SEA REGION

6TH EDITION

Print: ISSN 2668-7984, ISSN-L 2668-7984
Online: ISSN 2668-8115, ISSN-L 2668-7984
DOI: 10.55535/RMT.2024.4

Authors assume full responsibility
for the content of the published articles,
under Law no. 206 on 27.05.2004

COPYRIGHT: Articles may be reproduced free of any charge, on condition that appropriate credit is given by making mention of the edition and date of the publication.

SECURITY STUDIES AND MILITARY SCIENCE INTERNATIONAL CONFERENCE,
ORGANISED BY THE DEFENCE STAFF

NOVEMBER 2024

INTERNATIONAL SCIENTIFIC COMMITTEE

Assoc. Prof. Greg SIMONS,
Department of Communication Science, Turiba University

Sergei KONOPLYOV,
Visiting Lecturer in Public Policy, Harvard Kennedy School of Government

Julian PAWLAK,
Research Associate, Helmut Schmidt University & German Institute for Defence and Strategic Studies

Ioanna LEKEA,
War Games Laboratory, Hellenic Air Force Academy, Athens

Prof. Plamen BOGDANOV,
University of Library Studies and Information Technologies, Sofia, Bulgaria

Assit. Prof. Vinko ŽNIDARŠIČ,
University of Defence, Republic of Serbia

Robert SZABOLCSI,
Obuda University, Budapest, Hungary

Miroslaw SMOLAREK,
"General Tadeusz Kosciuszko" Land Forces Academy, Wroclaw, Poland

Dariusz SKORUPKA,
"General Tadeusz Kosciuszko" Land Forces Academy, Wroclaw, Poland

Karl PRONHAGL,
Theresian Military Academy, Wiener Neustadt, Austria

Árpád POHL,
Faculty of Military Science and Officer Training, Budapest, Hungary

Assoc. Prof. Harald GELL, PhD,
Chairman of EU Military Erasmus Programme, Theresian Military Academy, Austria (expertise: military education and training)

Assoc. Prof. Taner ALBAYRAK, PhD,
Piri Reis University, Istanbul, Türkiye (expertise: maritime security, strategy and geopolitics at the Black Sea)

Bonita JACOBS, PhD,
University of North Georgia, Atlanta, USA

Prof. Stefano GEUNA,
Universita Degli Studi di Torino, Torino, Italy

Prof. Jaromir MARES, PhD,
Brno, the Czech Republic

Prof. Pavel OTRISAL, PhD,
Brno, the Czech Republic

Assoc. Prof. Dipl.
Jozef PUTTERA, BEng, CSc,
Armed Forces Academy of "General Milan Rastislav Stefanik", Liptovsky Mikulas, Slovakia

Assist. Prof. Antonia COLIBĂȘANU, PhD,
Department of International Relations and European Integration, National School of Political Studies and Public Administration, Romania

Larry WHITE, PhD,
lecturer in American and International Law, University of Economics and Technology, Ankara, Türkiye

Assoc. Prof. Iulian CHIFU, PhD,
Security and Defence Faculty, "Carol I" National Defence University, Romania

Florian CÎRCIUMARU, PhD,
Director, Centre for Defence and Security Strategic Studies, "Carol I" National Defence University, Romania

Dan-Lucian PETRESCU, PhD,
Centre for Defence and Security Strategic Studies, "Carol I" National Defence University, Romania

Scientific Researcher II
Cristian BĂHNĂREANU, PhD,
Centre for Defence and Security Strategic Studies, "Carol I" National Defence University, Romania

Scientific Researcher II
Mirela ATANASIU, PhD,
Centre for Defence and Security Strategic Studies, "Carol I" National Defence University, Romania

Scientific Researcher III Daniela LICĂ, PhD,
Centre for Defence and Security Strategic Studies, "Carol I" National Defence University, Romania

Scientific Researcher III
Crăișor Constantin IONIȚĂ, PhD,
Centre for Defence and Security Strategic Studies, "Carol I" National Defence University, Romania

Prof. Cristian-Octavian STANCIU, PhD,
Command and Staff Faculty, "Carol I" National Defence University, Romania

Assoc. Prof.
Florentina-Loredana DRAGOMIR, PhD,
Security and Defence Faculty, "Carol I" National Defence University, Romania

Prof. Marilena MOROȘAN, PhD,
Command and Staff Faculty, "Carol I" National Defence University, Romania

Assoc. Prof. Daniel ROMAN, PhD,
Command and Staff Faculty, "Carol I" National Defence University, Romania

Assoc. Prof.
Ștefan Antonio DAN-ȘUTEU, PhD,
Command and Staff Faculty, "Carol I" National Defence University, Romania

Assoc. Prof. Adi MUSTAȚĂ, PhD,
"Carol I" National Defence University, Romania

Assoc. Prof.
Lucian-Valeriu SCIPANOV, PhD, BEng,
"Carol I" National Defence University, Romania

Assoc. Prof. Cătălin CHIRIAC, PhD,
Command and Staff Faculty, "Carol I" National Defence University, Romania

Mădălina GHIBA, PhD,
Head, International Humanitarian Low Center, "Carol I" National Defence University, Romania

Assoc. Prof. Andi Mihail BĂNCILĂ, PhD,
"Ferdinand I" Military Technical Academy, România

Prof. Ghiță BÂRSAN, PhD, BEng,
Rector, "Nicolae Bălcescu" Land Forces Academy, Romania

Assoc. Prof. Aurelian RAȚIU, PhD,
"Nicolae Bălcescu" Land Forces Academy, Romania

Assoc. Prof. Dumitru IANCU, PhD,
"Nicolae Bălcescu" Land Forces Academy, Romania

Assoc. Prof. Laviniu BOJOR, PhD,
"Nicolae Bălcescu" Land Forces Academy, Romania

Prof. Dorel BADEA, PhD, BEng,
"Nicolae Bălcescu" Land Forces Academy, Romania

Prof. Paul TUDORACHE, PhD,
"Nicolae Bălcescu" Land Forces Academy, Romania

Assoc. Prof. Alexandru BABOȘ, PhD,
"Nicolae Bălcescu" Land Forces Academy, Romania

Assoc. Prof. George BUCĂȚA, PhD,
"Nicolae Bălcescu" Land Forces Academy, Romania

Assoc. Prof. Ionuț Alin CÎRDEI, PhD,
"Nicolae Bălcescu" Land Forces Academy, Romania

Assist. Prof. Annamaria SÂRBU, PhD,
"Nicolae Bălcescu" Land Forces Academy, Romania

Assist. Prof. Tiberiu GIURGIU, PhD, BEng,
"Nicolae Bălcescu" Land Forces Academy, Romania

Prof. Dănuț MOȘTEANU, PhD, BEng,
"Nicolae Bălcescu" Land Forces Academy, Romania

Prof. Sorin PÎNZARIU, PhD,
"Nicolae Bălcescu" Land Forces Academy, Romania

Prof. Mihai-Marcel NEAG, PhD,
"Nicolae Bălcescu" Land Forces Academy, Romania

Prof. Mircea VLADU, PhD,
"Nicolae Bălcescu" Land Forces Academy, Romania

Prof. Gheorghe MINCULETE, PhD,
"Nicolae Bălcescu" Land Forces Academy, Romania

Prof. Toma PLEȘANU, PhD, BEng,
"Nicolae Bălcescu" Land Forces Academy, Romania

Assoc. Prof. Ioan-Gabriel POPA, PhD,
"Nicolae Bălcescu" Land Forces Academy, Romania

Assoc. Prof. Romana OANCEA, PhD,
"Nicolae Bălcescu" Land Forces Academy, Romania

Assoc. Prof. Diana RANF, PhD,
"Nicolae Bălcescu" Land Forces Academy, Romania

Assoc. Prof. Marius MILANDRU, PhD,
"Nicolae Bălcescu" Land Forces Academy, Romania

Assoc. Prof. Ștefania BUMBUC, PhD,
"Nicolae Bălcescu" Land Forces Academy, Romania

Assist. Prof.
Crenguța-Mihaela MACOVEI, PhD,
"Nicolae Bălcescu" Land Forces Academy, Romania

Assoc. Prof. Hortensia GORSKI, PhD,
"Nicolae Bălcescu" Land Forces Academy, Romania

Assoc. Prof. Anca Georgeta DINICU, PhD,
"Nicolae Bălcescu" Land Forces Academy, Romania

Assoc. Prof. Alina CIUHUREANU, PhD,
"Nicolae Bălcescu" Land Forces Academy, Romania

Assoc. Prof. Alexandru STOIAN, PhD,
"Nicolae Bălcescu" Land Forces Academy, Romania

Assoc. Prof. Gabriel MĂNESCU, PhD,
"Nicolae Bălcescu" Land Forces Academy, Romania

Assoc. Prof. Isabela DRAGOMIR, PhD,
"Nicolae Bălcescu" Land Forces Academy, Romania

Assoc. Prof. Sabin GUȚAN, PhD,
"Nicolae Bălcescu" Land Forces Academy, Romania

Assoc. Prof.
Sebastian-Emanuel STAN, PhD,
"Nicolae Bălcescu" Land Forces Academy, Romania

Assoc. Prof. Constantin ANDREI, PhD,
"Nicolae Bălcescu" Land Forces Academy, Romania

Assoc. Prof. Brândușa NICULESCU, PhD,
"Nicolae Bălcescu" Land Forces Academy, Romania

Assoc. Prof. Georgel OPREAN, PhD,
"Nicolae Bălcescu" Land Forces Academy, Romania

Assoc. Prof. Leontin STANCIU, PhD,
"Nicolae Bălcescu" Land Forces Academy, Romania

Assist. Prof. Daniel SOLESCU, PhD,
"Nicolae Bălcescu" Land Forces Academy, Romania

Assist. Prof. Maria-Lucia RUSU, PhD,
"Nicolae Bălcescu" Land Forces Academy, Romania

Florin Alexandru PAVEL, PhD,
"Nicolae Bălcescu" Land Forces Academy, Romania

Prof. Adrian LESENCIUC, PhD,
"Henri Coandă" Air Force Academy, Romania

Assist. Prof. Rita PALAGHIA, PhD,
"Henri Coandă" Air Force Academy, Romania

Prof. Ion CHIORCEA, PhD,
"Mircea cel Bătrân" Naval Academy, Romania

Assoc. Prof. Romeo BOȘNEAGU, PhD,
"Mircea cel Bătrân" Naval Academy, Romania

Scientific Research II
Cristina BOGZEANU, PhD,
Mihai Viteazul National Intelligence Academy

Prof. Ioan BONDREA, PhD,
Rector, "Lucian Blaga" University, Romania

Prof. Claudiu-Vasile KIFOR, PhD,
Prorector, "Lucian Blaga" University, Romania

Prof. Lucian-Ionel CIOCA, PhD,
"Lucian Blaga" University, Romania

Prof. Adrian CURAJ, PhD,
UEFISCDI, Romania

Prof. Ion POPA, PhD,
University of Economic Studies, Romania

Prof. Cosmin DOBRIN, PhD,
University of Economic Studies, Romania

Prof. Florin Eduard GROSARU, PhD,
Regional Department of Defence Resources Management Studies, Romania

Prof. Cezar VASILESCU, PhD,
Regional Department of Defence Resources Management Studies, Romania

Assoc. Prof.
Maria CONSTANTINESCU, PhD,
Regional Department of Defence Resources Management Studies, Romania

Assoc. Prof. Aura CODREANU, PhD,
Regional Department of Defence Resources Management Studies, Romania

Assoc. Prof. Vlad DUMITRACHE, PhD,
Regional Department of Defence Resources Management Studies, Romania

Assist. Prof. Brîndușa POPA, PhD,
Regional Department of Defence Resources Management Studies, Romania

Assist. Prof. Cristina ANTONOAIE, PhD,
Regional Department of Defence Resources Management Studies, Romania

Teodora GIURGIU, PhD,
National Military Archives of Romania

Iulian BOȚOGHINĂ, PhD,
Central Archive Repository,
National Military Archives of Romania

Assist. Prof. Sorina-Georgiana RUSU, PhD,
Urban and Landscape Design Department,
"Ion Mincu" University of Architecture and Urban Planning

Assoc. Prof. Alexandru LUCINESCU, PhD,
Institute for Political Studies of Defence and Military History

CONTENTS

Mircea BARAC	9	Foreword
		MILITARY THEORY AND ART
Florin NISTOR Lucian Valeriu SCIPANOV	10	On the Maturity of Operational Art in Romanian Military Thinking
George-Ion TOROI	26	The Persistent Effectiveness of Decoys in Land Forces' Operations – Lessons From The Russian-Ukrainian Conflict –
Ionuț-Iulian CĂLUGARU	50	Defining the Current and Foreseeable Operating Environment and the Role of the Romanian Armed Forces on the Eastern Side of the North Atlantic Alliance
Ana-Maria MERLUȘCĂ Cristian-Octavian STANCIU	72	Theoretical-Practical Incongruences of Logistic Support in the Fight for the Conquest of Kyiv
Claudiu Valer NISTORESCU	86	Operation Kursk – Advantages, Risks, and Development Prospects for the Ukrainian Armed Forces –
Cristian PANAIT	102	The Importance of GEOINT in Supporting Military Actions in Ukraine
Valentin-Marian TOMA	112	The Use of Unmanned Systems in Maritime Confined Spaces
George-Ion TOROI	126	Integration of First Person View (FPV) Unmanned Aerial Systems in Romanian Ground Forces Operations
Florina Ghindescu COSTAȘ Roland Iosif MORARU Ioana-Raluca ADOCHIEI	150	Emerging Technologies and Challenges in Hybrid Unmanned Aerial Vehicle Operations in The Metaverse Era
Alexandru-Lucian CUCINSCHI	166	Table Top Assessment Games – A Method for Analysing Future Capabilities –
Iurii CIUBARA	178	The Evolution and Role of Cooperation for Organizing and Conducting Military Operations
Iulia BORISOV	192	Maskirovka – The Art of Deception à la Russe
		INTELLIGENCE AND SECURITY
Iulian CHIFU	208	Worst-Case Scenarios for a Turbulent World – Modelling How Far and How Costly Defence and Security Could Go –
Vasile-Dumitru RAȚIU	220	Adaptation of NATO to the New Realities from Allied Eastern and Southern Flanks
Violeta VASILEVA Veselina ALEKSANDROVA GAGAMOVA	232	Application of NATO Models for Building Information Infrastructure in Crisis Situations
Marian-Valentin BÎNĂ	248	Cyber Warfare – The New Theatre of War and Its Legislative Clarifications –
Claudiu-Cosmin RADU	256	The People's Republic of China and the Threats to NATO's Cyber Security
Claudia LASCATEU Mihai CONSTANTINESCU	278	Cyber Defence Strategies in the Healthcare Sector: Deterrence, Resilience, and Critical Infrastructure Protection
Grudi ANGELOV	294	National Doctrine and Strategy – Basis for the Nation's Success
Romeo BOȘNEAGU	304	The Mines War in the Black Sea: An Unfinished Conflict
Nehridzhan Arif MEHMED	318	Recruitment and Selection of Human Resources in Today's Dynamic Environment – Definitions, Features and Trends –
Galina TODOROVA	330	Human Resources and Their Motivation When Choosing a Military Profession
Desislava MADZHAROVA	340	Effectiveness of Civilian Oversight of the Security Sector through Parliamentary Committees
Marinela-Luminița Emanuela ZLATEA Alexandra-Lavinia HOROBEȚ Eugen Constantin ROȘCA	350	Energy Resilience during Armed Conflict: Reconsidering Hydrogen for European Union Energy Security
Petko DIMOV Georgi MARINOV	368	Digital Literacy and Resilience against Disinformation among NATO Military Personnel
Iulian DINULESCU	380	The Nordic Resistance Movement as a Threat to European and International Security
Ridvan Bari URCOSTA	398	The Red and Blue: The Soviet General Staff's Wargames (1940)
Daniel Ionel Andrei NISTOR	424	Strategic Communication – Essential Tool in Support of Romania's National Security in the Current Geopolitical Context
Carmen-Maria MOISE Irina TĂTARU	442	Security Risks between Analysis and Assumptions
Ioan-Sebastian BUDUROI	460	The Kosovo Precedent – Similar Effects on Other States. Case Study: Georgia and Ukraine
Oana-Elena BRÂNDA	480	Türkiye – Navigating Roles as an Uncomfortable Actor or Regional "Balancer" –
Adriana SAULIUC	492	The Middle East in the Face of a Perfect Storm – The Regional Impact of Israel-Hezbollah Conflict
Romeo BOȘNEAGU	504	Russia-Ukraine War of Drones – Strategic Impact, Tactics, and Implications. The Drones Dropped in Romania during the Russia-Ukraine War –
Grudi ANGELOV	522	National Strategy – Linkage between National Ideal and National Interests –
		DEFENCE RESOURCES MANAGEMENT
Cezar VASILESCU Aura CODREANU	532	Bridging the Gap between Analysis and Prediction – Towards the Development of an Integrated Predictive Model for Hybrid Threat Risk Assessment –
Dorel BADEA Diana Elena RANF Elisabeta-Emilia HALMAGHI	562	Using TTX as an Educational Tool in the Field of Integrated Defence Resource Management

Gabriel MĂNESCU Dumitru IANCU	572	The Strategic Relevance of National Defence Industry in Major Defence Planning Documents – A Contextual Approach –
Cătălin ANDRUȘ Ștefan SĂVULESCU Lucian IVAN	590	Analysis of the Defence Industry of the Russian Federation – Impact on the National Security of Romania –
Romică CERNAT	606	Directed Energy Weapons – Component of Disruptive Emerging Technology with Implications on Strategic Stability
Valentin-Marian IORDACHE Oana BORDIANU Iasmina Georgiana SAUCIUC	624	The Importance of Defence Intelligence in Ensuring Aviation Security within the Air Transport System
George BUCĂȚA Paul TUDORACHE	634	The Effects of Deglobalization in the Formation of a New Regionalized World from a Military Perspective
Ecaterina HLIHOR	656	Public Diplomacy in the Era of Artificial Intelligence – Opportunities and Challenges in Promoting Security in International Politics –
Theodor-Eugeniu MIHAI	672	Civilian Preparedness for Crisis Situations and the Development of Security Culture in Romania
Tiberiu GIURGIU Ioan VIRCA Gabriel NOJA	684	Military Mobility in the Vision of NATO and European Union
Adrian IURA	698	Cost Architecture – Financial Challenges in Implementing National, NATO and EU Security Policies and Strategies –
Silvia STANCIU	716	Blueprints for Change – Benchmarking Gender Dynamics within NATO and EU –
		MILITARY HISTORY
Valeria BĂLESCU	730	Romania and the USSR between the Spectre of War and Diplomacy in the Early 1930s
Andi Mihail BĂNCILĂ	754	Political, Economic, and Military Cooperation between Romania and the Successor States of Former British Rhodesia (Zambia and Zimbabwe) between 1970 and 1989
George UNGUREANU	768	Political-Diplomatic Regroupings and Military Implications at the Black Sea (February-October 1939)
Daniela Florentina BORCAN	796	Nicolae Titulescu and His Foreign Policy Implications for the Black Sea Security
Artur LEȘCU	802	Military Action in Securing and Restoring Order during the Pogroms in Bessarabia in 1903 and 1905
Ovidiu PĂDURARIU	812	Lessons Learned by the Romanian Armed Forces after the 1916 Military Campaign

FOREWORD

Colonel Mircea Barac

In the context of the 21st century complex challenges, the Black Sea Region remains a strategic area of utmost importance for global security and regional stability. The geopolitical dynamics, the emergence of new types of threats, as well as the need for solid international cooperation between the littoral states and their partners underline the significance of a permanent dialogue between experts, servicemen and political decision-makers.

This volume gathers the papers presented at the **2024 Romanian Military Thinking Conference**, having as central theme **"Defence and Military Cooperation Strategies for Ensuring Security in the Black Sea Region".** The conference was conceived as a platform for academic, professional and strategic dialogue, with the aim of bringing to the fore innovative solutions and perspectives related to the complex security challenges in this region of major geopolitical importance. Through its dual format – academic, based on scientific articles, and expert-level debates –, the event provided an environment conducive to reflection, analysis and exchange of ideas on the most topical issues regarding defence and military cooperation.

The conference was held at a time marked by multiple international crises, which highlighted the importance of a concerted effort to ensure a stable and predictable security environment. During the debates, essential topics were addressed, such as: the adaptation of defence strategies to the new geopolitical realities, the relevance of regional cooperation within alliances and strategic partnerships, the modernization of the armed forces and the integration of emerging technologies in the military field.

The Black Sea region has become, in recent years, an area of intense interaction between local, regional and global interests, marked by asymmetric risks and threats, frozen conflicts and strategic competitions. In this context, the debate on defence strategies and military cooperation has become key to strengthening resilience and promoting stability.

The papers in this volume reflect the diversity of perspectives and solutions suggested by experts from various fields, representatives of national and international institutions, as well as practitioners with extensive expertise in managing security issues. Through the quality of the ideas expressed, the present volume is intended to be not only a synthesis of the conference conclusions, but also a starting point for future research and initiatives in the field of security and defence.

We are grateful to all the participants who, through their efforts, contributed to the success of the event and to the development of the volume! We are convinced that the presented ideas and conclusions will constitute a valuable reference point for experts in the field and for all those interested in the Black Sea Region security issues!

ON THE MATURITY OF OPERATIONAL ART IN ROMANIAN MILITARY THINKING

Associate Professor Florin NISTOR, PhD
"Mircea cel Bătrân" Naval Academy, Constanța, Romania
Professor Lucian Valeriu SCIPANOV, PhD
"Carol I" National Defence University, Bucharest
DOI: 10.55535/RMT.2024.4.01

Going through the scientific military analyses of the ongoing Russian-Ukrainian and Middle Eastern wars, one can see their reference to a ubiquitous paradigm – the operational art. Within this approach, the authors intend to capture the philosophy of the concept of "operational art" through doctrinal introspection and the influence of the international schools on Romanian military thinking. It highlights the importance of operational art as a planning tool for a modern thinking school. The authors have traced the premises of the emergence, development, use, and doctrinal adaptation of the main characteristics of the concept related to the development of military art. This is also the purpose of this article, on the one hand, to promote and campaign for a deeper understanding of the concept, and on the other hand, to find a solution for the cognitive institutionalization of operational art (for example, a scientific centre). Thus, this paperwork does not aim for an exhaustive approach to the operational art but aims at briefly presenting the general progress of the operational art, as well as the evolution throughout Romanian military history. Interspersed with examples of how to apply it and of the effects it produces, the approach may arouse interest in paying more practical and theoretical attention to this important concept.

Keywords: military science; operational art – theory and practice; great tactics; minor tactics; operational art department;

INTRODUCTION

Operational art is a fairly well-known concept in Romanian military academics. On the one hand, it is an old legacy from Romania's modern military history. On the other hand, it represents a creative tool for approaching modern warfare, today being part of the Euro-Atlantic philosophy regarding the decision-making and implementing the process in military actions.

The advantage lies in the fact that, internationally, there is sufficient bibliography and, at the same time, the concept of operational art is approached thoroughly and scientifically in the university environment and the relevant conferences. Likewise, the military organizations, headquarters, and the decision-making process respect the requirements, principles, and methods specific to the operational art.

Although both the format of military planning manuals and doctrines promote elements of operational art, the authors believe that it is quite likely for this concept not to be fully understood by all participants involved in planning, executing, and evaluating military actions. Without speculating, in the best of circumstances, there are differences in understanding between officers of different services or specialties, ranks, and, of course, personnel in the multinational military environment. Having a large art component, the art of applying theoretical principles through the creativity of military commanders and planners, there is the premise that the way of understanding and applying the principles of the concept is different from one generation to another, from one school of thinking to another, from practitioner to theoretician, from planner to executor and so on.

Because this work is theoretical, historical examples are used for authentic arguments in the analysis of the concept of *"operational art"*.

In this context, the present paperwork is intended to bring back to attention the importance of operational art, this indispensable link between strategy and tactics. In addition, it is aimed at promoting it in the hope that the personnel directly and indirectly involved in the planning and execution of military actions will deepen and assimilate more knowledge about this very abstract concept, reducing the reluctance of some commanders and staff to apply a process that has proven its value in many operations, including in Ukraine.

Through this approach an introspection within the philosophy of operational art is proposed to be carried out by capturing the need for the emergence, development,

use, and doctrinal adaptation of its main characteristics and principles. To this end, the action aspects that foreshadowed the emergence, definition, and conceptual development of the doctrinal content of military art and the operational art's foundation will be considered.

The first objective of this paperwork is to present the main historical sources that sensed, predicted, generated, and developed operational art elements, which later defined the philosophy of modern operational art concepts. In addition, certain characteristics specific to operational art that have been applied in some military actions will be briefly presented. In this context, it will be possible to present the first national efforts to promote and develop operational art, by identifying the main Romanian authors who have supported the development of military art, in general, and of operational art, in particular.

Another goal is an enthusiastic attempt to promote a deep understanding of the operational art, the use of appropriate language, not only theoretically, according to manuals or doctrines, but also practically, as creative as possible in exercises.

The result of the research should support the understanding of this planning tool by all specialists, and the promotion of modern operational art at the military decision-makers level. Therefore, it could support the acceptance and development of knowledge in the field, based on the arguments presented in this article, and especially the conviction that a structure for research and exploitation of operational art is needed in the military system.

The authors' vision consists in the constructive application of critical thinking, the avoidance of harmful biases in the decision-making process on scientific foundations, and the argumentation that supports the promotion of the operational art in higher military educational institutions, at the level of field and operational command. Thus, operational art will be able to occupy its well-deserved place in the Romanian military thinking and will complete the spectrum of operational planning tools in the field of military art and science.

OPERATIONAL ART – FROM THE CONCEPT EMERGENCE TO ITS DEVELOPMENT IN INTERNATIONAL MILITARY THINKING

This chapter will present some historical sources on the emergence, place, role, and development of operational art, highlighting the fact that this component of military art adjoins strategy and tactics as the main tool for planning military actions at the operational level.

The authors point out and insist on differentiating the concepts *"operational art"* and *"operational level"*. Thus, they mention that operational art is not a tool

strictly dedicated to joint commands, while some confuse the joint level with the operational level. In the context of the above, operational art can be used, as appropriate to the situation, at both tactical and strategic level as well.

In order to comprehend the role and place of operational art in military thinking, the symbiotic relationships between the main concepts specific to military science will be presented. Thus, *military science* is a sphere of human activity whose function is to acquire and systematize the knowledge concerning the laws and principles of warfare, the rules and forms of organization, training and use of armed forces, the methods and procedures of military operations (*Probleme fundamentale ale ştiinţei militare*/Fundamental Problems of Military Science, 2004, p. 7).

Military art represents a specialized field of military science regarding the organization and management of armed combat and includes not only the principles, methods, procedures, tactics and rules of preparing and conducting military actions, but also the abilities of commanders and troops to achieve success in military actions. Military art is defined by its structure: the *theory of military art* (the technology of armed combat) and the *armed combat* (the conduct of military actions).

Operational art is a component of military art and represents the art of skilfully applying the principles of armed combat according to the acquired knowledge and experience of the commander, adapted to the conditions of military actions and other variables in the field.

It is obviously difficult to accurately define operational art. For example, in the American literature, the definition of the concept has been comprehensively surmised by Milan Vego, who emphasized that operational art is *"a component of military art concerned with the theory and practice of planning, preparing, conducting, and sustaining campaigns and major operations aimed at accomplish strategic or operational objectives in a given theatre"* (Vego, 2009, p. I-4.). The model envisioned by Vego is based on the *means-ways-ends* triptych.

It should be mentioned that even the words used throughout time have been different. For instance, the formulas of the time, used in the military art to define its levels, were: *Great Tactics (grand tactics)* and *Minor Tactics*.

❖ *Grand Tactics* or *General Tactics* – a concept that today represents a part of both *Strategy* and *Operational Art* (a formula used today for the campaign planning process – strategic level); in *Grand Tactics*, the problems concerning the coordination of the actions of the participating forces were solved through a rigorous evaluation of two essential factors: time and movement (today's manoeuvre). This problem

is very effectively addressed in today's military actions through operational design, chronization matrix and other planning documents (targeting, logistics).

❖ *Minor Tactics* or *Elementary Tactics* – the concept that today represents *tactics* (the related formula, used for the process of planning battles or clashes, representing the *tactical level*).

Following Napoleon's model of how to approach battles, it could be seen as a direction of development of a planning level different from the strategic level (General tactics). Napoleon envisioned an intermediate level of command and control of tactical forces in order to achieve his strategic goals (he foresaw the operational level as we know it today). One can see in his actions that the specific principles of tactical level planning (forces and means, means-ways-ends) were in place: the ends were established, the means were established (even if they were tactical level ones), but the ways were not well founded. The creative genius of the general identified a way for tactical forces to be engaged in large-scale military actions, by respecting principles of armed combat such as mobility, flexibility, surprise, coordination, concentration of effort, as well as elements of operational design such as centre of gravity (COG), line of operations (LO), vulnerabilities, decisive conditions (DC), decisive points (DP) etc. Even if not all of them were explicitly named, they are found in the great Napoleon's conceptions.

Napoleon's concept of using multiple corps required him to consider many of the principles of operational-level planning from the perspective of a strategic thinker. Forces were placed under a local command, assigned to a general on the ground (foreshadowing the development of the *mission command* concept). The missions of the corps were directed towards the same objective in order to achieve the end state set by Napoleon himself.

For planning, he foresaw and used coordination, synchronization, manoeuvre and logistical support. They, at the scale of military actions conducted by multiple forces, diverse in terms of equipment and specialization, prove the need to define an intermediate level of the application of military art, which would link the strategic level of the generals and the tactical level of the executive commanders. This level is represented by the operational level of military art, whereas the way of applying the principles of military art defines the concept of operational art as it is known today.

Such an approach, in terms of implementing the principles of military art at the operational level, is proof that the command and control of large, corps-level tactical units acting individually in different areas required the development

of operational-level thinking, which converges and demonstrates the emergence and need for the development of modern operational art.

Another important step in the emergence and recognition of the place of the operational level in the military art was determined by the development of the railroad (Tylecote, 1992) and, with it, the advent of the telegraph (Gray, 1892, pp. 639-659). The railroads exponentially increased the mobility of troops (Crump, 2007). The telegraph facilitated the transmission of orders and instructions in a very short time to any command at appreciable distances.

A further important moment in the development of operational art was marked by the First Industrial Revolution (18th-19th century). Mass production generated an adaptation of the war industry to the new innovations, so that weapon factories adopted the technologies, adapted to the need for supply in the flow of materials and armaments, shaped the logistic support lines by positioning themselves as close as possible to the areas of operations (Lynn, 1993, pp. 9-30), but sheltered from enemy actions, all of which influenced the way of perceiving and understanding how to wage war according to principles adapted to these realities, thus pertaining to operational thinking, the precursor of operational art specific principles.

An important turning point in the development of the operational art was the emergence of thinking schools generated by the establishment of staff and planning teams based mainly on battlefield experience, as well as on the vision of military strategists to implement their command-and-control vision according to the forces available, the expected effect and the enemy reaction.

Furthermore, it is worth mentioning the military personalities who significantly contributed to the emergence and evolution of modern operational art.

Gerhard von Scharnhorst (1755-1813) was tasked with reorganizing the Prussian army and establishing the Prussian General Staff. He also developed a comprehensive reform programme, centred on replacing the long-standing professional army (mercenaries) with a standing army based on universal service (conscripts).

Helmuth von Moltke (1800-1891), Chief of the Prussian General Staff (1857-1888), carried out major reforms in the doctrinal, structural and action-oriented approach to military art. The results of these reforms led to: the emergence of mass armies; the constant expansion of the battlefield; the emergence of the theatre of operations; the narrowing of the scope of military strategy; new methods of employing combat forces; war games at the tactical and strategic levels, as well as the execution of large-scale exercises and manoeuvres, measures that produced visible effects in the evolution of military art (Roth, pp. 7-8).

Antoine-Henry de Jomini (1779-1869) is the leading representative of the French school of thinking. Jomini's major contribution to the art of war was the application of the principles of armed combat. In his conception, the fundamental principles defining warfare concerned the manoeuvre of forces and means, the main effort, the concentration of effort, decisive points, centres of gravity, and lines of communication (de Jomini, 2012).

Carl von Clausewitz (1780-1831) uses the term *war plan* synonymously with a *military strategy* to refer to a mechanism that links the government to the commander and his forces (https://www.militarystrategymagazine.com/article/strategy-war-and-the-relevance-of–carl-von-clausewitz/). In his view, a war plan defines the objective of the use of military force and determines the appropriate means to achieve it. In Clausewitz's understanding, the term *war* describes a state that is initially characterized by a duel, whereas at the level of combat, it describes the interactive process of imposing one's will on the opponent, who in turn wishes to do the same. The basic ideas of warfare conveyed in his work are the use of appropriate means, the concordance between aim, objectives and means, probability, chance, the genius of the commander and the military virtues of the army (Ib.)

Clausewitz proposes several steps for the study of the factors (and their properties) that significantly impact the character and direction of war, such as: assessment of the strategic situation and identification of ways to carry out the political will; definition of goals, final objectives and courses of action; estimates of probabilities and opportunities in a war, discussion of courses of action and suitable contingencies; summarizing the results of a war plan (Ib.) As a result of the above, Clausewitz's work can be said to be a prerequisite for the revival of strategic thinking and action through the use of principles of operational art – this is an example of the use of operational art at the strategic level.

Summarizing, *Grand Tactics* involved how troops would be engaged and deployed, *Minor Tactics* included the integration of infantry, artillery and cavalry for a combined attack, and engineering focused on attacking and defending fortifications.

The emergence of the *operational level* and *operational art* concepts came after the mentioned approaches, as a result of the acknowledgement of the separation of the strategic level into two components of military art – the *strategic level (political-military level)* and *the operational level (military level of planning and leadership).*

Mikhail Tukhachevsky (1893-1937) is one of the first military specialists who mentioned the particular component elements of operational art, but without really

identifying the concept; it was an intuitive act generated by direct observation of the evolution of the physiognomy of war (https://cersipamantromanesc.wordpress.wordpress.com/tag/batalia-varsoviei/). *"Owing to the fact that it is impossible, with such extensive fronts in the modern age, to destroy the enemy in a single blow, we are obliged to do so gradually, through operations that cost the enemy more than ourselves. In short, a series of destructive operations must be carried out based on logical principles and successively planned with precise objectives in pursuit of the enemy's destruction. This mode of action can take the place of decisive battle, which was the form of engagement of armies in the past that fought on small-sized fronts".* (Tukhachevsky). It is obvious that Tukhachevsky later influenced the military art, being the one who suggested the existence of the operational level of planning and command.

Alexandr. A. Svechin (1878-1938) embodied Tukhachevsky's thinking and materialized the concept of *operational art (operativnoye iskusstvo)*, (Nistor 2017, p. 69, apud Durham, 1998, p. 3), by developing the concepts of *action/deep battle (glubokiy boy)* and *deep operation (glubokaya operatsiya)* (Glantz, 1989, pp. 31-43). Later, the USSR developed these concepts, transformed and refined in the Soviet combat regulations, which were achieved by actions of penetrating the front, encircling the strongest enemy group (today, referred to as the centre of gravity/COG) and annihilating it.

The concept prefigured, since its inception, the joint approach to warfare, the theory and practice of preparing and executing land, sea and air military actions. Operational art deals with the planning and execution of joint and independent operations (combat actions) at the strategic-operational, operational, and operational-tactical levels (Kozlov, 1971).

The application of these principles can be seen in the modern military actions, which followed the emergence and development of the concept and which validated the importance of operational art and the adaptation of the principles of military art to the new conditions of warfare. We exemplify some of these events with recommendations for further study, such as Gallipoli (Battle of Gallipoli, 19 February 1915-9 January 1916); Battle of Jutland (31 May 1916-1 June 1916); Operation Weserubung (April-June 1940) and the list can go on.

Finally, the role and purpose of each of the means used at each level of warfare could be mentioned. Thus, *strategy* determined *how, why, with whom, when* and *where* to use military force in military operations. *Operations* level dealt with the implementation of strategic directions in relation to the forces at the disposal

to produce effects at the strategic level. *Tactics* dealt with the execution of tasks to achieve operational objectives, whereas *logistics* had the role of providing troops at the front. Therefore, all the functions of logistics are included here.

THE OPERATIONAL ART IN ROMANIAN MILITARY THINKING

The first elements of *great tactics* (the name of the time for what we recognize today as operational art) are said to be found in the young Prussian officer, Carol I, the first King of Romania (1839, Sigmaringen – 1914, Sinaia). Although the king did not benefit from von Moltke's great reforms, the Prussian military school and the experience of the Second German-Danish War of 1864 supported the construction of the new Romanian army and influenced the tactics of the Independence War. The king's participation in the assault on the citadels of Fredericia and Dybbøl in Denmark in 1864 seems to have inspired him at Plevna, applying very cautious and intelligent tactics (https://historia.ro/sectiune/general/razboiul-de-independenta-al-romaniei-in-scrisorile-637676.html), a moment in which, without the participation of the Romanian Army, the Russians would have been defeated.

Today, it can be said that the most representative theorist and practitioner of the time regarding the *grand tactics* was Marshal Alexandru Averescu (3 April 1859, Babele, United Principalities – 2 October 1938, Bucharest, Romania). Having studied in Italy, he wrote three valuable tactical volumes. Although accused of translating and taking over some texts from foreign works (Otu, 2019, p. 18), the volumes became the bibliography of the Superior War School, of which Averescu became the commander, between 1864 and 1896. The tactics introduced in the military education by Averescu will define the fighting style of the Romanian Army in the First World War. We recall some combat actions defined by the *Great Tactics*: the Rusciuc attack of the Romanian Navy, the Flămanda Manoeuvre (exceptional action planning) (Scipanov, 2018, pp. 56-65), the Mărăști offensive (the fastest offensive pace in the war) and the list can go on.

A brilliant application of Grand Tactics was achieved in the Romanian-Hungarian war, where General Gheorghe D. Mărdărescu1 (4 August 1866, Iași, Romania – 5 September 1938, Bad Nauheim, Germany), former commander of the Superior War School, defeated the Hungarian Bolshevik army, occupying Budapest. The battle of 24 and 25 July 1919 (Tisa/Szolnok) is one of the most brilliant victories of the Romanian Army in the Hungarian Campaign after the First World War (https://mvu.ro/razboiul-de-dupa-marele-razboi-campania-din-ungaria-din-1919/

[1] General of the Romanian Army/General of Hungary (1919-1920), A.N.

and https://www.aktual24.ro/batalia-de-pe-tisa-si-ocuparea-budapestei-victoria-asupra-ungariei-care-a-facut-romania-mare-singurul-razboi-castigat-de-romani-singuri-fara-ajutorul-altor-aliati/). Gheorghe D. Mărdărescu mentioned: *"When the Hungarian Bolshevik army had crossed the Tisa..., in its blind arrogance it believed that the road to Transylvania had been opened. Confident in your tried valour, I directed you to attack the enemy's army in flank and rear. That is what happened! You flawlessly executed my orders, overcoming with manliness and bravery all obstacles that stood in your way. Through your bravery, soldiers of the manoeuvre group, you greatly contributed to the opening of the road to Budapest!"* (Furduiu, https://horthymiklos.wordpress.com/gheorghe-d-mardarescu/).

In Chapter II of the book *The Evolution of Operational Art: From Napoleon to the Present* (Olsen, van Creveld, 2010), the authors capture the spectacular evolution of German operational art: *"The Recovery: From Sitz to Blitz"* (as it is known, the blitzkrieg was at that time the most effective form of application of the operational art) (Showalter, pp. 35-63). Since Romania was an ally, we rather participated in losing the blitzkrieg in the USSR instead of learning to apply modern tactics. But the implementation of the writings of Frunze[2], Tukhachevsky, and Svechin, officers of the new Soviet school of operational art, made Operation Uranus (Battles of the Don Elbow/Stalingrad), led by Marshal Zhukov[3], turn the tide of the Second World War.

During the Communist period, we benefited from the Soviet teachings on operational art, with the desire to attack at the decisive moment and time, where the enemy least expects it and at his critical points. In this context, the impact of operational art on the Romanian military school was not surprising, those theories were applied in the Romanian Armed Forces, but under a specific language and a different philosophy.

After joining NATO, the Romanian Armed Forces naturally adopted the allied concepts, through a process that was not always easy or carried out easily, even NATO going through a process of strategic and operational redefinition. For example, the American school of thinking in 1961 was not a follower of this concept – *"...the purpose of this innovation (operational art) is unclear... in Western military science, operational art, as a theoretical concept, is completely rejected... The West must not add this concept to the harmony of military thinking"* (General Walter Jacobs, commander in the U.S. Army, 1961).

[2] Mikhail Vasilievich Frunze (1885, Pišpek, Russian Empire – 1925, Moscow, Russian S.F.S., USSR) was a Bolshevik leader during the Russian Revolution of 1917, A.N.

[3] Gheorghi Konstantinovich Zhukov (1896, Russian Empire – 1974, Moscow, Russian S.F.S., USSR) was a Soviet military and politician, A.N.

It was not until 1982, that the U.S. Army revived the German term of *operation*, and in 1986 the term of *operational art* was adopted by the Russians (FM 100-5). A decade later, in the U.S. Navy and U.S. Marine Corps doctrines since 1994, the term *operation* reappeared and the *operational level* and *operational art* were adopted.

The term *"manoeuvre approach"* is a form of manifestation of the British operational art. For example, the U.S. Marine Corps defined operational art as: *"the destruction of enemy cohesion through a variety of rapid, concentrated, and surprising methods"* (Vego, 2009, p. I-5). The examples can continue with forms of manifestation, such as Network Centric Operation, Effect Based Operation, NATO Effect Based Thinking etc., the operational art being, thus, a framework for the manifestation of military genius, supported by benchmarks, principles, procedures, and processes, models and lessons learned acquired over decades.

Allied doctrine states that operational art is essential in the process of planning the operation through the ability, imagination, creativity, and intuition to plan and carry out the deployment and use of forces, joint capabilities, and other means, in a series of military actions conducted in time and space, for the fulfilment of objectives and the achievement of the desired final state (COPD, Comprehensive Operations Planning Directive, NATO).

The national doctrine adopts the philosophy of the allied concept and emphasizes in the same way: *"Operational art consists in skilfully employing the military instrument to achieve strategic and operative objectives, through the design, organization, integration, and management of campaigns, operations"* (Doctrina Armatei României, 2012, p. 76); *"The operational art is based on the ability of a commander to solve complex and unstructured problems and to create a logical and clear framework, in some cases intuitive, which facilitates the process of planning and transmission of orders".* (Ib., p. 77).

Regarding the adaptation of the concept to the military actions of the Navy, it was included in the doctrinal approaches of the Romanian Navy: *"The content of maritime operational art includes the theory of preparing and conducting maritime operations and activities to ensure the area of action of the navy"*. (Curs de artă militară, 1998). A more up-to-date approach: *"Operational art consists in skilfully employing the military instrument in time and space, within a campaign/operation, to transpose the received strategic/operational objectives into actions executed at a tactical level, to achieve the final state."*; *"Operational art can be described as the creative application of the imagination of commanders, supported by own and the staff skills, knowledge and experience, to plan campaigns, major operations,*

and battles." (FN-2, 2018, p. III-30). *"One of the main purposes of the Operational Art is to plan the battle in the most favourable terms possible so that the enemy can be put at a disadvantage. A brilliant tactic can rarely replace an inadequate operational art".* (Vego, p. I-11). In light of what has been presented, it can be summarized that the Romanian thinking school adopted the concept. Thus, creatively applying operational art is the key to comprehensive and effective planning to achieve victory in military action in the shortest possible time and with minimal losses.

From the point of view of the use of operational art, many such examples can be found in the analyses of the Russian-Ukrainian war, and a few can be mentioned that the authors recommend for reading.

For example, retired General Ben Hodges, former commander of the United States Army Europe, analyses the miracle of the counteroffensive in Kharkiv Oblast through the lens of operational art: *"... because of the combination of things I talked about – the deception, the discipline, the preparation. What we have seen so far is operational art".* (https://kyivindependent.com/retired-us-general-if-russia-used-nuclear-weapon-in-ukraine-us-would-have-to-get-directly-involved/).

In *Wavell Room* magazine, Chris Hughes, in the article *Operational Art Reborn*, analyses Russia's action from the point of view of operational art: *"Russia's consistent failure to practice the barest outlines of operational art during the planning and execution of their ‹Special Military Operation› must rank among the foremost explanations. Poor campaign planning, a failure to consider contingencies, and an inability to logically sequence and focus actions supporting a clear strategic main effort saw it squander any opportunity it may have had to impose a fait accompli in Ukraine"* (https://wavellroom.com/2024/01/12/operational-art-reborn-part-one/; https://wavellroom.com/2024/01/12/operational-art-reborn-part-two/).

Along the same line, at the West Point[4] Academy, works such as *Back to the Future: Rediscovering Operational Art in an Era of Great Power Competition* can be identified, in which pertinent analyses of war through the lens of operational art can be found (https://mwi.westpoint.edu/back-to-the-future-rediscovering-operational-art-in-an-era-of-great-power-competition/).

The Japanese school itself, through Yasuhiro Kawakami[5], addresses the Russian-Ukrainian war in the article *"Dissecting Russia's Operational Art in Ukraine. How Disjointed Ends, Ways, and Means Have Shackled Moscow's Operational Warfare"*

[4] United States Military Academy West Point.

[5] Security expert specialized in military strategy, operational mobility, tactics, national defence studies and Japanese security policy, A.N.

(https://www.spf.org/iina/en/articles/kawakami_02.html) and examples can continue by simply searching the internet.

In Romanian military thinking, the specialized study stands out: *"Convențional și hibrid în primul an al războiului Federației Ruse împotriva Ucrainei, concluzii și lecții desprinse din război"* (Ioniță, 2023), in which there are also some lessons identified at the operational level, a study that the authors recommend to be continued.

In the authors' opinion, Ukraine's undoubtedly use of the operational art in war was the key to the resilience of this country in the face of the Russian aggressor. The informational preparation for combat was correct and anticipatory (Joint Preparation of the Operational Environment/JPOE/done correctly – element of OA) and the Centre of Gravity (COG – the essence of OA) was correctly identified and protected during the first stages of the invasion (Force Protection – effectively carried out, element of OA), the Russian mechanized troops were lured into urban areas (deception – element of OA), mobile detachments, combined for ambushes were used (mission command – element of OA), and the Russian logistics lines were attacked (indirect approach – element of OA). When the culmination of the Russian special operation ceased, recognized from the moment when the aggressor forces did not fulfil their objectives (determination of the culmination – element of OA), the Ukrainian forces successfully began the counteroffensive on converging directions (coordination, synchronization, synergy – principles of OA). The authors opine that during the continuation of the offensive, Ukrainian forces had to apply the principle of surprise continuously. Ben Hodges suggested an indirect approach by building a bridgehead in Crimea (https://www.dw.com/ro/ucraina-ar-putea-elibera-crimeea-p%C3%A2n%C4%83-la-sf%C3%A2r%C8%99itul-verii-afirm%C4%83-generalul-american-%C3%AEn-retragere-ben-hodges/a-65279616).

The question that arises is *Where did the Ukrainian military leaders learn the operational art?* The answer is that they had learned it before, as the Russian heritage was capitalized upon in a Department within the National Defence University of Ukraine in Kyiv. Later, benefiting from the opening to the West, the classical Russian operational art was enriched with the Western one, contributing, it seems decisively, to the success of the Ukrainian forces. Another example is operational logistics, which is also a pillar of the OA. That is why the Ukrainians can request exactly what equipment and ammunition they need and when they actually need it.

CONCLUSIONS

This article attempts to promote this tool for planning and executing military actions – the operational art –, without an exhaustive review of the theory and practice of military art, but rather through specific examples that have marked the emergence and evolution of the concept. The authors envisage that each officer, as his or her career evolution progresses, should have a thorough knowledge of the fundamentals of operational art and apply it creatively, according to their character qualities, national particularities, traditions and ingenuity.

Operational art is a valuable tool for the commander and his staff to find ways to deal with the uncertainty and ambiguity of the increasingly complex, volatile and unpredictable theatre of operations.

Although it does not have a clear definition, which is an advantage, making it flexible, OA is rather a cognitive framework in which the genius of military thinking can manifest itself, which is why there are so many practical examples under the umbrella of a single concept. Thus, the role of operational art, as a tool for planning military action, does not provide one with infallible solutions, being a framework for critical and creative thinking that, under the springs of directional cues and lessons learned, helps inter-arms, inter-force, inter-governmental and multinational creativity.

Operational art is the only planning tool that combines tactical actions into a broader design to help achieve strategic objectives. The authors emphasize that tactical actions, even if successful, cannot lead to victory if they are not integrated into an operational concept.

One of the conclusions resulting from the place and role of operational art in the Romanian military thinking supports and justifies the importance of studying operational art in military institutions, especially in *"Carol I"* National Defence University, within master's programmes and postgraduate courses, together with elements of military art, in order to achieve the necessary connections to develop critical thinking in relation to their principles, thus promoting the ubiquity of operational art.

The final conclusion, from the authors' experience, is that although there is a relevant doctrinal maturity, the Romanian operational art is not at a stage of full maturity, which in fact represents its continuous development and transformation. Therefore, the recommendation is to consider the possibility of the existence of a research centre, department or interdepartmental centre of excellence,

headquartered in a military educational institution that would deal strictly with the issue of operational art, following the model existing in Ukraine and the main allied states.

BIBLIOGRAPHY:

1. Crump, Th. (2007). *A Brief History of the Age of Steam: The Power that Drove the Industrial Revolution*. London: Robinson. ISBN 978-1-84529-553-0. OCLC 213605104.
2. *Curs de artă militară* (1998). București: Academia de Înalte Studii Militare.
3. Course *"Probleme fundamentale ale ştiinţei militare".* (2004). Bucureşti: Editura U.N.Ap.
4. *Doctrina Armatei României* (2012). București, p. 76.
5. Durham, R.W. (1998). *Operational Art in the Conduct of Naval Operations*. Monograph in the U.S. Navy School of Advances Military Studies, Kansas, p. 3.
6. *FM 100-5*, U.S. Army Field Manual.
7. *FN-2, Manualul pentru organizarea de stat major şi planificare a operaţiilor în Forţele Navale* (2018). București, p. III-30.
8. Glantz, D.M., Col. (Dec. 1989). *Soviet Operational Maneuver in a Period of Reform*. In *Military Review*. Fort Leavenworth. Kansas, pp. 31-43.
9. Gray, Th. (1892). *The Inventors of the Telegraph and Telephone. Annual Report of the Board of Regents of the Smithsonian Institution*. 71: 639-659, http://books.google.com/?id=tnjfe4vEBGwC&pg=PA639, retrieved on 7 August 2019.
10. Ioniță, C.-C., BG (r.) PhD (2023). *"Convențional și hibrid în primul an al războiului Federației Ruse împotriva Ucrainei, concluzii și lecții desprinse din război"*. Centrul de Studii Strategice de Apărare și de Securitate. București: Universitatea Națională de Apărare *"Carol I"*.
11. De Jomini, A.-H. (2012). *Precis de l'Art de la Guerre. French edition*, https://medium.com/@defstudy/jomini-art-of-war-559d340582b6, retrieved on 12 August 2024.
12. Kozlov, S.N. (1971). *Officer's Handbook*. Defense Technical Information Center, translated from Russian in 1977, Washington, D.C.: Department of Defense, Department of the Air Force.
13. Lynn, J.A. (1993-b). *The History of Logistics and Supplying War*. In Lynn, J.A. (ed.). *Feeding Mars: Logistics in Western Warfare from the Middle Ages to the Present*. London and New York: Routledge, pp. 9-30.
14. Nistor, F. (2017). *Să redescoperim arta operativă maritimă*. București: Editura U.N.Ap. *"Carol I"*, p. 69.
15. Olsen, J.A. (ed.), van Creveld, M. (ed.) (2010). *The Evolution of Operational Art: From Napoleon to the Present.* Oxford University Press.
16. Otu, P. (2019). *Mareșalul Alexandru Averescu, militarul, omul politic, legenda*. București: Editura Militară, p. 18.
17. Roth, G. *Field Marshal von Moltke the Elder, His Importance Then and Now*, pp. 7-8, https://www.jstor.org/stable/26302811?seq=1, retrieved on 12 August 2024.
18. Scipanov, L.V. (2018). *The contribution of the Romanian sailors to military actions which imprinted the Romania's entry into First World War*. Bucharest: *"Carol I"* National Defence University Bulletin, no. 4, pp. 56-65.

19. Showalter, D.E. *Prussian-German Operational Art, 1740-1943*, pp. 35–63, https://doi.org/10.1093/acprof:oso/9780199599486.003.0003, retrieved on 10 August 2024.
20. Tylecote, R.F. (1992). *A History of Metallurgy*. Second Edition. London: Maney Publishing, for the Institute of Materials. ISBN 978-0901462886.
21. Vego, M. (2009). *Joint Operational Warfare – Theory and Practice*. U.S. Naval War College, Newport.
22. https://cersipamantromanesc.wordpress.com/tag/batalia-varsoviei/, retrieved on 6 July 2024.
23. https://historia.ro/sectiune/general/razboiul-de-independenta-al-romaniei-in-scrisorile-637676.html, retrieved on 8 July 2024.
24. Prof. Ilie Furduiu, https://horthymiklos.wordpress.com/gheorghe-d-mardarescu, retrieved on 22 July 2024.
25. https://kyivindependent.com/retired-us-general-if-russia-used-nuclear-weapon-in-ukraine-us-would-have-to-get-directly-involved/, retrieved on 4 July 2024.
26. https://www.militarystrategymagazine.com/article/strategy-war-and-the-relevance-of-carl-von-clausewitz/, retrieved on 11 July 2024.
27. https://mwi.westpoint.edu/back-to-the-future-rediscovering-operational-art-in-an-era-of-great-power-competition/, retrieved on 6 July 2024.
28. https://mvu.ro/razboiul-de-dupa-marele-razboi-campania-din-ungaria-din-1919/, retrieved on 22 July 2024.
29. https://www.dw.com/ro/ucraina-ar-putea-elibera-crimeea-p%C3%A2n%C4%83-la-sf%C3%A2r%C8%99itul-verii-afirm%C4%83-generalul-american-%C3%AEn-retragere-ben-hodges/a-65279616, retrieved on 22 July 2024.
30. https://wavellroom.com/2024/01/12/operational-art-reborn-part-two/, retrieved on 22 July 2024.
31. https://www.spf.org/iina/en/articles/kawakami_02.html, retrieved on 4 July 2024.

THE PERSISTENT EFFECTIVENESS OF DECOYS IN LAND FORCES' OPERATIONS – LESSONS FROM THE RUSSIAN-UKRAINIAN CONFLICT –

Lieutenant Colonel Senior Instructor George-Ion TOROI, PhD

"Carol I" National Defence University, Bucharest, Romania

DOI: 10.55535/RMT.2024.4.02

The ongoing war in Ukraine has changed the nature of armed conflict. Among other things, it has demonstrated that today's unprecedented technological developments have led to much greater risks to the protection of forces on the battlefield. The extensive use of unmanned aerial systems, both for fire control and especially for battle space reconnaissance, has made the battle environment extremely transparent. As a result, armed forces have had to find effective ways of protecting their own forces and operations. One of these measures has proven to be the use of decoys to mislead enemy forces and attack systems. The purpose of this article is to provide a comprehensive picture of the operational necessity of such methods and to offer recommendations based on the lessons learned in Ukraine, where both belligerents have made extensive use of such methods. I anticipate that these findings will contribute significantly to a deeper understanding of the implications of false targets in contemporary military operations.

Keywords: decoy; deception; operational advantage; protection; operating environment;

Motto:
"Seeing more on the battlefield doesn't necessarily imply understanding what's truly unfolding".

Mick Ryan

INTRODUCTION

Russia's invasion of Ukraine through the *"special military operation"* (UN, 2022), which began on 24 February 2022, was a turning point in international relations worldwide. The world entered an era of fierce competition (Joint Doctrine Note 1-19 Competition Continuum, 2019, p. 1; Mazarr-1, 2018, p. 1; Mazarr-2, 2022, pp. 111-113; MCDP 1-4 Competing, 2020, pp. 1-3), with most actors moving towards accelerated armament. After a long period of peace, high-intensity military operations have returned to a Europe seemingly unprepared for them. This change has created new challenges and threats for European states, including Romania. The recalibration of security and defence policies has become a priority in the current context. However, it is still unclear how it will be implemented.

Beyond the atrocities inherent in any conflict and the suffering of those involved, the conflict in Ukraine has been and continues to be an inexhaustible source of lessons for adapting the structure of armed forces and the way conflicts are conducted. From inaccurate planning based on faulty assumptions due to self-interest, to the use and destruction of weapon systems, the Russian-Ukrainian conflict has revealed many important aspects of adapting armed forces to today's challenges. They should constitute the framework for adapting the security and defence policies of European states, including Romania.

Problem Statement

The Russian-Ukrainian war provides valuable lessons about the nature of contemporary conflicts. One of the lessons is that in a highly transparent environment, combined with the development of strike technologies much deeper into enemy territory and much more accurate, and an extremely shortened strike cycle from the moment of target confirmation, solutions for force protection must be found. This context has highlighted the importance and effectiveness of deception in modern military operations as a strategy of deception, and the conflict

offers a number of lessons that can support the adaptation of military forces. It is recognized that *"the return to great power competition against peer adversaries with advanced anti-access/area-denial (A2AD) capabilities* ***requires a renewed focus on the use of deception****"* (Hays, 2020, p. 56). The numerous examples of decoys in the ongoing Russian-Ukrainian conflict demonstrate the effectiveness and relevance of this deception technique in the current operational context.

However, most Western militaries, including Romania's, seem to have abandoned this approach in favour of heavily arming themselves with modern combat systems. The operational comfort provided by air and information superiority until the beginning of this decade has led to the loss of this art from the repertoire of Western armies. Another reason for the lack of interest in decoys in most Western militaries is that they are often seen as useless devices in today's operational environment, where highly sophisticated means of detection give the impression of increased transparency in the battlefield. However, as the Australian General Mick Ryan recognized, seeing more does not necessarily mean understanding more (Ryan, 2024), the way in which the Ukrainians have managed to deceive the Russians, who have such advanced intelligence-gathering sensors, is a testament to this.

Therefore, the research problem that lies at the basis of this scientific endeavour is the lack of training of Western military forces, including Romania's, in the effective use of decoys as a means of achieving force protection.

Research Objectives

In line with the research problem presented above, the main objective of this study is to identify certain lessons learned from the conflict in Ukraine that can be implemented by the Romanian Armed Forces in their efforts to adapt to the challenges of the current operational environment.

Thus, the study provides an in-depth analysis of the persistence of the effectiveness of decoys in military operations, based on the lessons learned from the ongoing conflict in Ukraine. By analysing in detail how they have been used in this conflict, the study also aims to provide a broader perspective on their effectiveness in contemporary military operations.

In this context, we pursue a number of secondary objectives, as follows:

- identify the operational benefits of using decoys in military operations;
- highlight the key challenges and opportunities presented by the current operational environment for the use of decoys;

- interpret the concept of false targeting in the context of the theory of deception;
- identify and interpret instances of the use of decoys in the Russian-Ukrainian conflict.

Although the results of the study can be applied to all armed forces, they are mainly addressed to the Romanian Army. This is *the target of this research*. Moreover, I would like to emphasize the *main limitation of the research*, which is the use of only the information circulated in the public space, a limitation imposed mainly by the information protection measures taken by the two belligerents, given that this conflict is still ongoing.

Research Methodology

The conducted study is a qualitative one, attempting to capture the full range of implications regarding the use of decoys in the current operational context. I would like to mention that the proposed objectives are those that have guided this chosen approach. Accordingly, the study does not aim to test hypotheses, but the research questions are those that direct the study towards the fulfilment of the proposed objectives. These are as follows:

❖ *What are the operational benefits of using decoys in military operations?*

❖ *What challenges and opportunities do the current operational environment present for the use of decoys?*

❖ *How do decoys fit into the theory of deception?*

❖ *What lessons can be drawn from the Russian-Ukrainian conflict on the use of decoys?*

The research strategy is a case study to identify the key elements that have contributed to the effectiveness of deception in the military operations in the conflict in Ukraine, using secondary data due to the impossibility of direct access, one of the challenges of ongoing military conflicts.

Paper Structure

The paper is divided into three parts in terms of objectives and research questions. Thus, the first part analyses, from a theoretical point of view, the concept of *decoy*, the advantages it can offer in the design of operations, and the opportunities and challenges that the current operational environment offers for this approach. I then analyse how decoys work from the perspective of deception theory, and finally examine a number of examples from the conflict in Ukraine to identify valuable operational lessons for the purpose of this study.

DECOYS – CONCEPT, BENEFITS, CHALLENGES AND OPPORTUNITIES

The modern battlefield is characterized by a multitude of threats and challenges for the armed forces. The saturation of the battlefield with sensors and technological devices that allow constant monitoring of troop movements and military equipment has become a reality in today's conflicts, requiring constant adaptation and innovation of military strategies. It has become increasingly difficult to conceal military intentions and actions. In this respect, a concept that has proven its usefulness over the years, that of deception, has returned to the attention of military specialists in response to these challenges, in order to ensure the survival and effectiveness of armed structures in the new conditions of combat. The persistent effectiveness of decoys in military operations is a topic of great interest in the current context of the Russian-Ukrainian conflict. However, as mentioned in the identified research problem, it is insufficiently considered by the Romanian Armed Forces.

Concept

First, I recognize that the definition and basic concepts associated with decoys are essential to understanding their role in military strategies. For this reason, this section is devoted to a theoretical analysis of the importance and use of decoys in military operations.

In the context of military operations, the term decoy refers to *"an imitation of a person, object, or phenomenon intended to deceive the enemy's surveillance or detection systems and thereby mislead the enemy"*. (FM 1-02.1 Operational Terms, 2024, p. 21; AAP-06, 2021, p. 39). Tactical ground decoys are therefore fictitious devices designed to deceive enemy observers by simulating one or more vehicles, artillery, radar, combat installations, or other items of interest to the enemy such as bridges, buildings, or various communication routes.

Decoys have always played a crucial role in armed conflict. There are countless historical examples of their use. The most famous dates back to the Second World War, as part of the Allies' Operation *Quicksilver*, to deceive the Germans about the true location of the Normandy landings. It involved the creation of a fictitious force, the 1st US Army Group, to be perceived by the enemy as a real threat. The location of this fictitious force was set in the south-east of England, *"poised"* to invade Europe through the Pas-de-Calais, the most logical option from the German point of view.

This fictitious force was even mentioned in German documents, demonstrating the viability of the strategy. The use of fake military equipment, such as inflatable tanks or wooden planes, was instrumental in shaping the Nazi perception of the Allied landing zone. The power of deception to influence the conduct of military operations can never be underestimated.

Operational Benefits

Decoys can make a significant contribution to **maintaining a high level of operational capability** of military forces by diverting the enemy's attention away from high-value targets. A Chinese study shows that a 1:1 ratio between real and decoy targets can reduce the losses of military units by up to 40%, and a 3:1 ratio in favour of decoys by 50% (Information warfare gives rise to a camouflage revolution, 2012). It can therefore be seen that false targets play a crucial role in achieving force protection by providing the adversary with alternative targets, thus reducing his chances of engaging the real ones.

In addition, the use of decoys can contribute to **increasing the adversary's uncertainty** about the operational situation, which can lead to decision-making errors on the adversary's side. In this way, decoys exploit one of the constant characteristics of warfare throughout history, namely uncertainty. Because of this specific aspect of the nature of conflict, decoys have been, and continue to be, a practical and relatively inexpensive way to gain tactical advantage on the battlefield. Moreover, their use can ensure that the adversary is misled about the organization, combat strength and intentions of the force. By creating a superior numerical picture of one's own forces, decoys can even help deter certain enemy actions.

Decoys can also be used to **draw attention to certain operationally irrelevant areas or targets** by increasing the illusion of their importance, thereby facilitating freedom of movement for friendly forces at times and in areas critical to mission success.

In addition, decoys can be used to **attract the enemy's attention and force him to reveal his position and intentions**. This strategy is extremely useful in creating vulnerabilities for the enemy and successfully destroying some of his critical equipment.

Reducing an adversary's warfighting capability by causing him to waste resources destroying targets that are in fact false is a major benefit of decoys and can significantly influence the conduct of military operations in the long term.

The same Chinese study mentioned earlier shows that a 3:1 ratio in favour of decoys can increase the enemy's consumption by 70% (Ib.). Moreover, maintaining an adversary's confusion about the effectiveness of its strike capabilities can contribute to increasing the chances of achieving surprise, as it may cause the adversary to redeploy its resources inefficiently, placing them in a position of operational vulnerability.

False targets can also be used to **ensure the replacement of military equipment in the contact area**, creating the illusion that the force in question is still in position, when in fact it is ready to intervene in another area. It can facilitate the surprise effect of the adversary, thereby increasing the tactical effectiveness of military operations.

In addition, the proven efficiency of decoys can have a **positive impact on troop morale**, contribute to the achievement of military objectives, and be a **destabilizing factor for the adversary** by creating a climate of uncertainty and confusion.

In today's information age, where information has taken on new dimensions, the use of false targets can also be used as a **disinformation strategy** to confuse the adversary and create a false perception of the intentions and capabilities of one's own forces. Publicly promoting the success of one's own decoys on the battlefield will have a powerful psychological effect on the enemy, casting doubt on his future decisions.

As it has been demonstrated, there are a myriad of operational benefits that decoys can bring in support of military objectives, provided they appear credible to the adversary. In this respect, there are two **relevant factors** in enhancing the credibility of decoy targets, namely their fidelity and the operational significance of their exploitation.

Fidelity refers to the degree of realism of the target. A high-fidelity decoy must accurately reproduce the characteristics of the target it is imitating in electromagnetic space. It is not enough that it looks like the target, it must also have the appropriate thermal signature, the acoustic and electromagnetic emissions of the target, to effectively attract and manipulate the enemy. The operational importance of the decoy is how it fits into the image the deceiver wants to present to the adversary. The more it respects the real way of fighting, the more effective it will be. In this respect, it is important to consider the specific details of the construction of this image. For example, the camouflage of false targets, the positioning of decoys in the specific tactical operation or the creation of a realistic illusion of the environment

are essential aspects to make the use of decoys in support of military operations more effective. In order to increase the chances of success of decoys, it is essential that the above be consistent with the adversary's level of situational understanding.

Challenges and Opportunities in the Current Operating Environment

There are countless examples of the use of decoys throughout history. Regardless of the time period and social development, effective solutions have been found to develop them to a point where they can prove their operational effectiveness on the battlefield. However, today's unprecedented technological development puts additional pressure on their use in military operations. The ongoing conflict in Ukraine highlights the constant threat of unmanned aerial systems (UAS), indirect fire or electronic warfare (EW), all of which hinder the effective use of decoys in military operations. At the same time, the changing nature of conflict in today's operating environment provides a number of opportunities for the use of decoys to gain advantage over the enemy. This section briefly outlines the key challenges and opportunities for the role of decoys in today's operational environment.

Modern surveillance systems, such as advanced drones, satellites and radars, can more easily detect differences between decoys and real equipment, requiring the creation of highly realistic decoy targets, including simulated heat signatures and radio communications specific to the original. With the development and proliferation of electronic warfare capabilities, the electromagnetic signature of a decoy has become essential. It necessitates the need to gain superiority over the adversary's signature management to increase the chances of successful deception. (Ryan, 2024). Multi-spectral decoys can therefore provide an effective response to the challenges of the current operational environment, offering significant advantages in target simulation and adversary confusion. Today, ad hoc efforts to deceive the adversary, including the use of decoys, have become increasingly easy to detect and counter, so the importance of multi-spectral decoys has grown significantly. In this respect, adaptability and innovation must be the measure of operational success. In addition, to increase the credibility of decoys, it is essential to construct a compelling narrative for the adversary to achieve favourable results in attracting attention and misleading them.

In addition, the rapid pace at which contemporary conflicts are being transformed by the armed forces adaptability can pose a major challenge to the effective use of decoys. The conflict in Ukraine demonstrated the initial success of many capabilities (UAS Bayraktar TB2, HIMARS etc.), which were later countered

by countermeasures adopted by the opposing side as part of the adaptation process, significantly reducing their effectiveness. It also poses a challenge to the use of decoys, which must keep pace with changes on the battlefield in order to remain relevant. This requires continuous adaptation of both operational procedures and the technologies used to increase the fidelity of the replicas built.

However, the same operational environment can also present a number of opportunities to be exploited through the ingenious use of decoys. First, technological development can help improve the reliability of decoys. It can also provide the framework for the emergence of new ways and means of deception. For example, in the future *"decoys will have the ability to mask visual, thermal and radar wavebands and will be an integral part of defence systems. It should be technically feasible to have entire structures of* ***robotic decoys*** *for deception operations, but simple ones designed to mimic the electromagnetic signature of manoeuvre unit command posts are more likely to be developed in the near term".* (Science & Technology Trends 2020-2040 – Exploring the S&T Edge, 2020, p. 44). The reliance on military cyber structures may provide the framework for the development of cyber *"honeypot"* fake targets that can be used to lure and identify attackers.

Furthermore, regardless of the technological development of information-gathering sensors, the primary target of deception, and therefore decoys, is the human mind, which remains susceptible to deception. (Bennett, 2007, p. 12). Thus, constructing an image that matches the opponent's prior beliefs can ensure the successful use of decoys.

In addition, the rapid pace of change in the contemporary tactical environment has placed additional pressure on the need for rapid target engagement. Thus, shortening the identification-engagement cycle may prove to be an advantage in the modern use of decoys, which can more easily and effectively deceive enemy forces due to the reduced time imposed on collection systems for target confirmation.

INTERPRETATION OF DECOYS IN THE CONTEXT OF THE THEORY OF DECEPTION

The concept of deception is an integral part of the broad field of deception. Deception is the totality of actions taken to deceive the opposing force commander by manipulating his perception of the operational situation and eliciting a behavioural response that provides an advantage to the deceiver. (AJP3.10.2, 2020, p. 4; FM 3-13.4, Army Support to Military Deception, 2019, pp. 1-1). It can therefore

be seen that decoys fit the definition of deception perfectly. They are used to create an illusion of reality for the adversary and cause him to make incorrect decisions, which can result in one of the many operational benefits previously presented in this paper.

At its core, deception is a communication process between the deceiver and the target. The essence of the deception process is the presentation of certain observables to the adversary, which he can interpret in such a way as to form the desired perception of the deceiver, on the basis of which the expected response can be made. American doctrine describes this process in three steps: *"see – think – do"* (FM 3-13.4, Army Support to Military Deception, 2019, pp. 2-5).

Within this framework, the tools used to create the observables that the adversary must identify are what the theory calls the **means of deception**. They fall into three broad categories: physical, technical, and administrative. As far as false targets are concerned, referring to the definition given at the beginning of the first section of this article, we can say that they fall into the first stage of the American methodology, representing means of deception. They can be used to present the wrong message to the opponent, to manipulate his perception in accordance with the proposed objectives, in order to provoke a specific reaction, be it action or inaction. Thus, the use of decoys is intended either to induce the adversary to take an action that is actually unfavourable to him, or to induce him not to take an action that would be advantageous to him. In both cases, the intent is to manipulate his behaviour.

Decoys are essential tools in deception operations, supporting the manipulation of enemy perceptions and influencing enemy decisions during military operations. Their use supports most of the principles of deception as defined by R.V. Jones (Jones, 2013, p. 24), a renowned researcher in the field, as follows:

- fake targets can be used to deceive the enemy into believing that your forces are in a location other than the real one by placing them in the fake location so that the enemy is trapped or distracted from the real targets;
- fake targets may replicate weapon systems that are not in the force or are present in limited numbers to distort the adversary's perception of the number of forces and weapons held;
- presenting decoys in such a way that they appear to be protecting a particular area or about to take certain actions that threaten the adversary can attract the adversary's attention and resources when, in fact, the decoy intends to do something else;

- decoys can also create a false impression of the location and timing of the deceiver's future actions by focusing the adversary's attention on an operationally irrelevant area or time;
- the use of false targets may cause the adversary to misinterpret the nature of the deceiver's future tactical actions, leading the adversary to prepare or respond inappropriately;
- decoys can exploit the adversary's misconceptions about the deceiver's knowledge of the operational situation, potentially influencing the deceiver's decisions and causing him to alter his plans;
- the use of false targets can reinforce the impression of success or failure of the deceiver's actions, causing the adversary to misinterpret the operational situation and react inappropriately.

False targets also imply a high degree of versatility in terms of the concepts with which deception operates. Thus, in terms of their operational role, decoys can support **both A Type – ambiguity-producing deception (Type A) or M Type – misleading deception (Type M)** (Daniel, 1980, p. 8; FM 3-13.4, Army Support to Military Deception, 2019, pp. 1-6; JP 3-13.4, Military Deception, 2017, pp. I-9; MCTP 3-32F Deception, 2024, pp. 2-9). Leading the adversary to a particular decision by presenting false indicators is an effective strategy of using false targets to reduce the adversary's level of uncertainty. It involves exploiting his prior beliefs about a given situation and encouraging them by exposing decoys. As a result, the adversary will be inclined to choose the option that is actually advantageous to the deceiver. False targets can also be used to confuse the opponent. Public exposure of the success of such methods can create uncertainty and hesitation in the adversary's future decisions, which can help make the deceiver's actions more effective. It can be seen, therefore, that decoys can be considered an effective tool in the theory of deception, since they can be used for either creating or eliminating ambiguity, a crucial element in manipulating the recipient's reality.

In addition, since false targets are an element used to be observable and attract attention, their use can be achieved mainly through the **simulation method**. It involves creating objects or situations that suggest a certain reality in order to attract attention and mislead the receiver. Although less common because of their complexity and much higher risk, decoys can also be used through the other specific method of deception, **dissimulation**. While simulation involves the use of false targets, dissimulation is more complex. It involves first influencing the adversary's

perception of the success of the decoys and then, against this background, modelling real equipment that appears to him to be fake. As we have seen, it involves a higher degree of risk, but it can be a deceptive solution in extreme cases.

Given their nature, that of attracting attention, the use of fake targets is mainly achieved through **display** as a **specific tactic of deception**. It involves the simulation of equipment or actions to mislead the adversary as to the disposition, size, or intent of the forces initiating the deception. In this regard, decoys can be used to create the illusion of a situation that requires a particular response from the adversary.

The use of false targets can also help increase the effectiveness of misleading actions that employ other tactics. Thus, their appropriate use can ensure the credibility of a disinformation campaign or, by diverting the enemy's attention to other areas, ensure the concealment and camouflage of real forces and actions.

It can be seen that the analysis of deception theory highlights the versatility of the decoy concept in terms of its use in different operational contexts. Thus, false targets play a crucial role in supporting deception operations and contribute to shaping the enemy's perception of the tactical situation (Friedman, 2017, p. 76) and, consequently, its vulnerability.

OPERATIONAL LESSONS FROM THE USE OF DECOYS IN THE RUSSIAN-UKRAINIAN CONFLICT

In the current Russian-Ukrainian conflict, the use of decoys has been a particularly important technique used by both sides to gain tactical advantage. Understanding the nuances in which decoys have been used by the two belligerents can provide valuable operational lessons about the dynamics and complexities of modern warfare. For this reason, the first part of this section will examine the most significant examples of decoy use in the Russian-Ukrainian conflict. It should be recalled that the analysis is based exclusively on information that has been made public through open sources; classified information is not taken into account. However, I accept it as normal for an ongoing conflict in which each side has implemented OPSEC security measures to protect their technologies and deception strategies.

Examples of the Use of Decoys in the Russian-Ukrainian Conflict

The Ukrainian Army's use of decoys

A prime example dates back to the Battle of Kharkiv in May 2022. (Ukraine Deploys Gun-Toting Mannequins to Drive Russians from Kharkiv, 2022). The use

of mannequins to create the image of a larger Ukrainian force than in reality was intended to increase the threat level to the Russians. Even though they were relatively rudimentary, crudely equipped and armed with decorative weapons, they could have misled some Russian reconnaissance drones and been mistaken for real Ukrainian soldiers from a distance. The effectiveness of decoys in this conflict has been documented, with videos suggesting Russian artillery attacks on Ukrainian positions that appeared to be defended by such decoys (Rivero, 2024). These attacks demonstrated the effectiveness of diversionary tactics, using decoy targets to draw enemy fire and gain battlefield advantage. It is important to note that these decoys represented the role of improvisation and were not equipped with equipment specifically designed for military use, but were creatively used to enhance the tactical effectiveness of the Ukrainian forces, as can be seen in *figure 1*.



Figure 1: Mannequins used by the Ukrainian army
(Ukraine Deploys Gun-Toting Mannequins to Drive Russians from Kharkiv, 2022)

The use of dummies to protect high-value systems was another way in which the Ukrainian military implemented this tactic. Inflatable replicas of HIMARS systems have been instrumental in wasting expensive Russian capabilities designed to destroy them. A video posted on social media this year shows an Iskander missile costing around 3 million euros engaging such an inflatable system. (X, 2024). It is a concrete example of the effectiveness of decoys in operations carried out by the Ukrainian military. The importance and effectiveness of HIMARS systems in Ukraine's military operations has been proven in countless situations. Due to their outstanding performance, these systems have inevitably become high-value targets for Russian forces, who are aware of their power and destructive potential. This reality has significantly increased the need for their protection. Taking advantage of the Russians' desire to attack as many of these systems as possible,

as quickly as possible, the use of inflatable decoys, such as those produced by the Czech company *"Inflatech Decoy"* (Inflatech Decoy, 2024), has proven to be a crucial element in protecting HIMARS systems. The effectiveness of such decoys was also demonstrated by the fact that the Russians once announced that they had destroyed more systems than Ukraine had received from its allies. (Fact Check: Did Russia Claim it Destroyed 44 HIMARS Launchers in Ukraine?, 2022).

At the same time, Ukrainian forces have placed decoys throughout the depth of the Ukrainian lines in Kherson, Zaporizhzhia, and Donbass, representing replicas of various types of systems, whether Soviet or Western, such as M777 howitzers, D-20 or D-30 artillery systems, as well as other tanks or air defence systems, all of which represent high-value targets for the Russians (Rivero, 2024). To increase the credibility of these fake targets, they are equipped with signatures similar to the original – optical, radar or infrared. Moreover, also for this reason, they are mounted on towable platforms that ensure their deployability to increase Russian confusion. (Czech-made M270 MLRS inflatable decoy from Inflatech tricks Russian strike forces in Ukraine, 2024). *Figure 2* highlights a series of such decoys.



Figure 2: Examples of lures used by the Ukrainians, replicas of valuable systems
(compiled by the author)

In addition to providing protection, the Ukrainians have also used inflatable replicas of high-value systems to increase the threat level to the Russians. Placing such *"capabilities"* in close proximity to the contact has proven to be an effective and risk-free strategy to provoke a Russian response in order to minimize potential casualties in terms of human or material losses.

The efficiency of their use is also proved by the fact that one of the Ukrainian factories has directed its production to such decoys for the Ukrainian army. (Metinvest begins production of decoy military equipment that misleads the enemy, 2023). The efficiency of the products of the Metinvest factory is proven by the fact that more than half of the products delivered to the Ukrainian army have already been destroyed by the Russians. (Ukraine's Armed Forces Employ Decoys to Locate the Source of Russian Artillery Fire, 2023). In addition, in early March, images of a replica of the Sentinel anti-aircraft radar left behind by the Ukrainian forces after their withdrawal from Advika appeared on social media platforms. The degree of fidelity of the radar, allegedly built in this factory, was impressive, almost indistinguishable from the original. (X, 2024).

Moreover, the reproduction time of the systems is not very long. For example, an M777 howitzer takes about two weeks, while a Ukrainian D-20 artillery system takes only four days. (Ukraine's Armed Forces Employ Decoys to Locate the Source of Russian Artillery Fire, 2023). These replicas are built from simple and cheap materials, but are detailed enough to fool Russian troops and draw attacks to false targets. For example, one launcher is made from a piece of sewer pipe mounted on an old satellite dish. However, these replicas look quite real, as can be seen in *figure 3*.



Figure 3: M777 howitzer replica
(Metinvest begins production of decoy military equipment that misleads the enemy, 2023)

In addition, the construction of such replicas was used by the Ukrainians as an information operation (INFOOPS) in the fight against the Russians. Thus, they allowed teams of journalists to visit such a factory in order to document the degree of realism of the resulting products ('A psychological weapon': inside a Ukrainian factory making decoy kit, 2023). The visit and the positive impressions of the journalists were intended to create confusion and indecision among Russian decision-makers in future actions.

The Russian military's use of false targets

Russian forces have extensive experience in using false targets in armed conflicts, as the intervention in Ukraine demonstrates. They have been using this method since the beginning of the conflict. A prime example is the arrow-like devices used as decoys for Ukrainian anti-aircraft systems to protect its ballistic missiles, unknown even to the Americans (Russia Deploys a Mystery Munition in Ukraine, 2022). These devices are launched by Iskander-M missiles when they signal that Ukrainian anti-aircraft systems are being intercepted. Each device is equipped with electronic components and emits radio signals to jam or deceive enemy radars attempting to detect the Iskander-M missile. The device also contains a heat source to attract any projectiles attempting to destroy the missile. *Figure 4 (a;b)* highlights these devices used by the Russians as decoys.



Figure 4 a: Decoy devices for the protection of Iskander-M missiles (compiled by the author)

When the Ukrainians began attacking Russia's military airfields, Russia resorted to fake targets to increase the chances of survival of its own capabilities, but also to cause the Ukrainians to waste their already scarce resources (Africk, 2024). A telling example of such a Russian practice is the image depicting a helicopter landing on a fake fighter plane drawn on the runway (Epstein, 2024).



Figure 4 b: A fake fighter plane, drawn on the runway (Epstein, 2024; Africk, 2024)

Similar to the Ukrainians, the Russians used inflatable replicas of their own weapon systems, as shown in *figure 5*. They would place the decoys in such a way that they would be discovered by the Ukrainians, then, after a few days, they would replace them with real systems to ambush the opposing forces (Kazakova, 2023). This type of tactic proved to be highly effective, at least in the initial stages. Even after the discovery of the Russian method of using these fake replicas, their usefulness continued to be considerable, increasing the level of hesitation and making it more difficult for the Ukrainians to target. In addition, one of the challenges of the conflict in Ukraine, the protection of command posts, is also felt by the Russians. For this reason, they used inflatable bunkers to make the Ukrainians waste their ammunition (Rivero, 2024).



Figure 5: Russian inflatable models (S-300 on the left and T-80 on the right) (Kazakova, 2023)

Another instance of the Russians using false targets was during the Ukrainian counteroffensive in the Zaporizhzhia region in the summer of 2023 (Kofman, 2023). In this case, the Russians, being on the defensive, used some of their own trenches

as bait for the Ukrainians. They planted explosives in these trenches, which they would detonate remotely when the Ukrainians went in to clear them (Khurshudyan, 2023). Moreover, for the purpose of wasting Ukrainian resources, the Russians used inert X-55 rockets to attract the attention and fire of Ukrainian anti-aircraft systems (Lisnichuk, 2022). Also out of this desire, the Russians used balloons with simple metal triangles suspended from them to appear as a missile or drone on Ukrainian radars. (Ukraine says it shot down 6 Russian balloons that appeared over Kyiv, 2023). It is worth noting the importance of these decoys, given that some anti-aircraft missiles supplied to Ukraine by Western allies can cost up to $4 million each (Sullivan, 2022).

A final relevant example of how the Russians used decoys was to increase the protection of bridges, critical elements for the mobility of their own forces and resources (Helfrich, 2022). They used radar reflectors to create a signature similar to the bridge, installed next to the bridge to attract Ukrainian missiles, as can be seen in *figure 6*.



Figure 6: The Russians' ghost bridge (Helfrich, 2022)

Operational lessons and recommendations

The examples presented above demonstrate the viability of the false target concept in contemporary military operations. In addition, they provide valuable lessons for adapting forces to the demands of today's operational environment, the most important of which can be summarized as follows:

❖ Even the most rudimentary decoys can be enough to deceive the enemy. The use of decoys by the Ukrainians to slow down Russian operations has shown

that they can be very effective in creating distraction and confusion among the enemy. Thus, the imaginative use of all available resources in support of military operations can be critical to force protection and mission success.

❖ However, to increase the chances of success, decoys must keep pace with technological developments. Technology has been, and will continue to be, the primary factor influencing the adaptation of combat tactics (Piehler, 2013, p. 362). It is also true for decoys, which must evolve technologically in order to be successful in their operational role. Their degree of fidelity must correlate with the adversary's intelligence gathering capabilities. Therefore, adapting decoys to the specific challenges of the operational environment is critical to their success. In this respect, decoys must replicate not only the visual, but also the thermal or radar signature of the targets, their acoustic characteristics, and their behaviour in order to maximize their effectiveness.

❖ To add to the enemy's confusion, decoys must also have built-in systems that mimic the fake target's explosion or even a possible fire response, making it more credible to the enemy. In this way, the adversary will be tempted to believe that he has hit a real target. It has at least two advantages. First, it will increase the protection of the decoys, which will lead the adversary to stop looking for the real targets, and second, it will create a distorted picture of the operational situation, which may contribute to his subsequent surprise.

❖ The emergence of new capabilities on the battlefield, such as autonomous combat systems (robots), will require the continuous adaptation of decoys to these technological developments. Serious analysis is needed both from the perspective of deception of such systems by constructed replicas and from the perspective of how robots can become potential decoys to attract enemy attention. Therefore, continuous adaptation to the specific challenges of the nature of armed conflict must be an essential requirement for their success in future military operations.

❖ The picture created by the use of decoys must be as realistic and complete as possible, but also consistent with the enemy's expectations of the operational situation. To achieve this goal, decoys must be placed in areas that make operational sense, and their placement and operation must be consistent with operational procedures. Special attention must also be paid to their camouflage, which must blend with the environment to create the most realistic illusion of the presence of friendly forces.

❖ Ingenuity in the use of decoys can ensure operational success. Examples include the use of fake replicas of HIMARS systems to induce the adversary to withdraw certain key capabilities or devote additional resources to their protection,

the use of trenches as decoys in defensive operations, or the use of fake devices to attract the adversary's expensive missiles.

❖ Decoys are an important asset in protecting high-value proprietary capabilities. Distracting the enemy and redirecting enemy attacks to false targets are effective strategies for misleading the enemy and protecting your assets. For example, in the context of today's conflict challenges, the use of decoys is critical to protecting own command posts. Command posts have been, and will continue to be, one of the most important enemy targets on the battlefield. Their destruction means disorganizing the enemy's forces, which will contribute to neutralizing his ability to coordinate his actions and respond effectively on the battlefield. Thus, the creation of false positions and structures, supplemented by systems imitating radio communications, the placement of false antennas imitating the communications system of the command post and inflatable vehicles can mislead the enemy into attacking these elements of great importance to him with expensive attack systems, wasting his own precious resources. This will also complement and help protect the deceiver's real command and control systems.

❖ Wasting the enemy's resources is one of the primary operational functions of deception. In a conflict of attrition such as the one in Ukraine, logistical support can be the decisive capability in winning or losing the war. For this reason, the effectiveness and adaptability of decoys used by military forces is essential to increase the chances of operational success.

❖ In the information age, when the main attribute of information has changed from knowledge to influence, the effectiveness of the use of decoys in the military actions of ground forces can be used as information operations, thus increasing the degree of indecision of the enemy in his future actions.

❖ Finally, it is absolutely necessary to monitor the effectiveness of one's own decoys and evaluate the enemy's reaction to them in order to ensure their adaptation to the existing operational situations. It is a truism that the effectiveness of decoys is determined by how quickly they are destroyed by the enemy.

CONCLUSIONS

The process of adaptation is essential to the survival of any organization, including the military. For this reason, it is crucial to identify the critical elements of the way in which the armed forces operate and to be able to transform in a timely manner. As the battlespace becomes increasingly transparent, the battle strategies and tactics employed to ensure force protection and mission security must be

constantly adapted. The use of decoys in military operations is a critical issue in this context, as they can provide a variety of operational benefits, as the ongoing conflict in Ukraine has so far demonstrated.

This study has analysed how these decoys have been used in the aforementioned conflict and can conclude that this art is far from dying out. On the contrary, its proven effectiveness shows how essential it is in modern military operations. Therefore, armed forces, including the Romanian ones, should consider paying much more attention to deception as a component of military operations. Some of the reasons can be considered as follows:

- firstly, not all potential adversaries have advanced ISR capabilities to cover the entire confrontation space;
- secondly, all ISR systems have some limitations. Many of them can process signatures in several spectrums, but never in the entire electromagnetic spectrum simultaneously;
- thirdly, it can take several days to validate targets, which could give an advantage to the use of false targets;
- fourthly, a single questionable element is sufficient to cause the adversary to become indecisive and to gain significant operational advantage;
- finally, precision munitions are extremely expensive and in short supply, so decoys can contribute significantly to the waste of valuable adversary resources.

Therefore, the Romanian Armed Forces should, inter alia, carry out the following activities in order to enhance their own capabilities for the effective use of false targets in military operations:

- develop doctrines and procedures for their integration during operations specific to each branch and service;
- train their own forces on how to use decoy integration during military exercises;
- integrate decoys into simulation exercises and war games;
- continually monitor technological developments and adapt their own decoys and specific operational procedures;
- test the effectiveness of own decoys;
- purchase prefabricated multi-spectral decoys. Their price is much lower compared to any real equipment;
- one procurement option would be to earmark part of the price of a particular weapon system, e.g. 1%, for the purchase or research development of its replicas;

- consider the establishment of a dedicated structure in the Romanian Armed Forces. The Russians continue to maintain the independent 45th camouflage regiment, one of whose tasks is the use of decoys.

In conclusion, I believe that the Romanian Armed Forces should increasingly incorporate the use of decoys in its military operations as a means of protecting own forces and actions in an increasingly transparent operational environment. It is also necessary to take advantage of the lessons learned from the current Russian-Ukrainian conflict, which provides the perfect risk-free environment for learning and adapting new tactics, techniques and procedures.

BIBLIOGRAPHY:

1. *'A psychological weapon': inside a Ukrainian factory making decoy kit* (4 September 2023), The Guardian, https://www.theguardian.com/world/2023/sep/04/a-psychological-weapon-inside-a-ukrainian-factory-making-decoy-kit, retrieved on 21 June 2024.
2. AAP-06. (2021). AAP-06, NATO Glossary of terms and definitions (English and French). NATO Standardization Office.
3. Africk, B. (9 June 2024). *Russia adds decoys to air bases near Ukraine*, https://read.bradyafrick.com/p/russia-adds-decoy-aircraft-to-air, retrieved on 22 June 2024.
4. AJP3.10.2. (2020). Allied Joint Doctrine for operations security and deception, edition A, version 2. NATO Standardization Office.
5. Bennett, M., Waltz, E. (2007). *Counter-deception Principles and Applications for National Security*. London: Artech House.
6. *Czech-made M270 MLRS inflatable decoy from Inflatech tricks Russian strike forces in Ukraine* (19 August 2024), Army Recognition, https://armyrecognition.com/focus-analysis-conflicts/army/conflicts-in-the-world/russia-ukraine-war-2022/czech-made-m270-mlrs-inflatable-decoy-from-inflatech-tricks-russian-strike-forces-in-ukraine?highlight=WyJkZWNveSJd, retrieved on 12 June 2024.
7. Daniel, D.C. (1980). *Multidisciplinary Perspectives on Military Deception*. Monterey, California: US Department of the Navy, United States Naval Postgraduate School.
8. Helfrich, E., Rogoway, T. (August 2022). *Russia Is Building 'Ghost Bridges' with Radar Reflectors in Ukraine*, The Warzone, https://www.twz.com/russia-building-ghost-bridges-with-radar-reflectors-in-ukraine, retrieved on 12 May 2024.
9. Epstein, J. (2 April 2024). *Russia's helicopters are screwing up its attempt to fool Ukraine with decoys by landing on its fake painted fighter jets: intel*, Business Insider, https://www.businessinsider.com/russia-helicopters-land-fake-fighter-jets-undermining-decoy-tactic-ukraine-2024-4, retrieved on 23 May 2024.
10. *Fact Check: Did Russia Claim It Destroyed 44 HIMARS Launchers in Ukraine?* (2 September 2022), Newsweek, https://www.newsweek.com/did-russia-claim-destroy-44-himars-launchers-ukraine-1739314, retrieved on 13 May 2024.
11. FM 1-02.1 Operational Terms. (2024). Washington D.C.: US Department of the Army.
12. FM 3-13.4, Army Support to Military Deception. (2019). Washington D.C.: US Department of the Army.

13. Friedman, B. (2017). *On Tactics. A theory of victory in battle*. Annapolis: Naval Institute Press.
14. Future Leadership. (2020). Multinational Capability Development Campaign.
15. Hays, M.G., LTC (2020). *Convergence of Military Deception in Support of Multi-Domain Operations.* In-Theater Army in Multi-Domain Operations Integrated Research Project. US Army War College.
16. Inflatech Decoy. (2024), https://www.inflatechdecoy.com/, retrieved on 23 May 2024.
17. *Information warfare gives rise to a camouflage revolution* (10 August 2012), https://news.sina.com.cn/o/2012-08-10/053924941796.shtml, retrieved on 22 May 2024.
18. Khurshudyan, I., Maslov, S., Hrabchuk, K. (6 August 2023). *Ukraine's elite forces rely on technology to strike behind enemy lines*, The Washington Post, https://www.washingtonpost.com/world/2023/08/06/ukraine-special-forces-alpha-counteroffensive/, retrieved on 23 May 2024.
19. JCN1/17. (2017). Joint Concept Note (JCN) 1/17 Future Force Concept. UK Ministry of Defence.
20. Joint Doctrine Note 1-19 Competition Continuum (2019). US Joint Chiefs of Staff.
21. Jones, R. (2013). *The 8 Principles of Security and the 8 Principles of Deception.* In B.W. Hy Rothstein, The Art and Science of Military Deception (pp. 23-24). London: Artech House.
22. JP 3-13.4, Military Deception. (2017). US Joint Chiefs of Staff.
23. Kazakova, O. (4 October 2023). *Fake howitzers and inflatable tanks: how else the Russian Armed Forces deceive the Ukrainian Armed Forces*, News.ru, https://news.ru/cis/falshivye-gaubicy-i-naduvnye-tanki-kak-eshe-vs-rossii-obmanyvayut-vsu/, retrieved on 23 May 2024.
24. Lisnichuk, M. (27 November 2022). *Bait for air defense of Ukraine: the Russian army began to launch more often inert cruise missiles X-55*, Oboz.ua, https://war.obozrevatel.com/primanka-dlya-pvo-ukrainyi-armiya-rf-nachala-chasche-zapuskat-inertnyie-kryilatyie-raketyi-h-55.htm, retrieved on 12 May 2024.
25. MCDP 1-4 Competing. (2020). U.S. Marine Corps.
26. MCTP 3-32F Deception. (2024). U.S. Marine Corps.
27. *Metinvest begins production of decoy military equipment that misleads the enemy*. (25 August 2023), Metinvest, https://metinvestholding.com/en/media/news/metnvest-rozpochav-virobnictvo-maketv-vjsjkovo-tehnki-scho-vvodyatj-voroga-v-omanu, retrieved on 12 May 2024.
28. Mazarr, M.J. et al.-1 (2018). *Understanding the Emerging Era of International Competition. Theoretical and Historical Perspectives*. Santa Monica, California: RAND Corporation.
29. Mazarr, M.J. et al.-2 (2022). *Understanding the Emerging Era of International Competition Through the Eyes of Others. Country Perspectives*. Santa Monica, California: RAND Corporation.
30. Kofman, M., Lee, R. (4 September 2023). *Perseverance and Adaptation: Ukraine's Counteroffensive at Three Months, War on the Rocks*, https://warontherocks.com/2023/09/perseverance-and-adaptation-ukraines-counteroffensive-at-three-months/, retrieved on 23 May 2024.
31. Piehler, G.K. (2013). *Encyclopedia of Military Science.* Los Angeles: Sage Publications.

32. Rivero, J.L. (April 2024). *Decoy Warfare: Lessons and Implication from the War in Ukraine*, US Naval Institute, https://www.usni.org/magazines/proceedings/2024/april/decoy-warfare-lessons-and-implication-war-ukraine, retrieved on 22 May 2024.
33. *Russia Deploys a Mystery Munition in Ukraine* (14 March 2022), The New York Times, https://www.nytimes.com/2022/03/14/us/russia-ukraine-weapons-decoy.html, retrieved on 13 May 2024.
34. Ryan, M. (2024), https://mickryan.substack.com/p/the-quest-for-a-new-offensive-doctrine, retrieved on 12 May 2024.
35. *Science & Technology Trends 2020-2040* – Exploring the S&T Edge (2020). Brussels: NATO Science & Technology Organization.
36. Sullivan, B., Bowman, T. (21 December 2022). *The U.S. will send a Patriot air defense system to Ukraine. How will it help?*, https://www.npr.org/2022/12/21/1144662505/us-ukraine-patriot-missile-system, retrieved on 17 June 2024.
37. TC 7-102. (2014). Training Circular No. 7-102 Operational Environment and Army learning. Washington DC: Headquarters Department of the Army.
38. The Jerusalem Post. (2023), https://www.jpost.com/international/internationalrussia-ukraine-war/article-762030, retrieved on 12 May 2024.
39. *Ukraine Deploys Gun-Toting Mannequins to Drive Russians From Kharkiv* (22 May 2022), Newsweek: https://www.newsweek.com/ukraine-deploys-gun-toting-mannequins-drive-russians-kharkiv-1706788, retrieved on 22 May.
40. *Ukraine says it shot down 6 Russian balloons that appeared over Kyiv* (16 February 2023), https://www.npr.org/2023/02/16/1157457205/ukraine-russia-balloons, retrieved on 22 May 2024.
41. *Ukraine's Armed Forces Employ Decoys to Locate the Source of Russian Artillery Fire* (3 October 2023), Metinvest, https://metinvestholding.com/en/media/news/zsu-vikoristovuyutj-maketi-schob-tochno-viznachiti-zvdki-strlya-rosjsjka-artilerya-reportazh-the-wall-street-journal-z-virobnictva-modelej-tehnki-vd-metnvestu-dlya-zsu, retrieved on 12 May 2024.
42. United Nations/UN (2022), *Russian Federation Announces 'Special Military Operation' in Ukraine as Security Council Meets in Eleventh-Hour Effort to Avoid Full-Scale Conflict*, https://press.un.org/en/2022/sc14803.doc.htm, retrieved on 22 June 2024.
43. *X.* (2024), https://x.com/Tendar/status/1788964161575116871?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1788964161575116871%7Ctwgr%5E772fe80018a0b64b0ab2815e69d01adb7662ce0b%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.digi24.ro%2Fstiri%2Fexterne%2Fcum-sa-irosest, retrieved on 23 May 2024.
44. *X*. (2 March 2024), https://x.com/bayraktar_1love/status/1763863165652070728, retrieved on 22 May 2024.

DEFINING THE CURRENT AND FORESEEABLE OPERATING ENVIRONMENT AND THE ROLE OF THE ROMANIAN ARMED FORCES ON THE EASTERN SIDE OF THE NORTH ATLANTIC ALLIANCE

Captain Ionuț-Iulian CĂLUGĂRU, PhD Student
"Carol I" National Defence University, Bucharest
DOI: 10.55535/RMT.2024.4.03

The character of the battlefield is becoming more nuanced and even different as new emerging and disruptive technologies are discovered and developed. Defining the operating environment as an integrating term for all that is represented by armed combat has been and will remain a necessity, especially now that the international defence system and, by consequence, the military system is experiencing a flood of innovative concepts.

The operating environment cannot be sufficiently defined without reference to the actors that participate and generate its dynamics. In this regard, we consider it necessary to provide a new perspective on the main forms of threats to the security of the North Atlantic Treaty Organization, in which we will focus the attention of this study on the security environment on the eastern side of the North Atlantic Alliance, with specific focus on highlighting the place and role that Romania has in the NATO architectural framework, aiming at the geostrategic area already mentioned.

In order to meet the above-mentioned objective, we will resort to methods specific to military sciences, such as historical analysis, study of documents and comparative analysis, aiming to validate the working hypothesis that Romania is a member that contributes essentially to NATO's defence mission in the current security environment and the threats to it, at present and in the future.

Keywords: NATO; operating environment; Romanian Armed Forces; security environment; technological development;

INTRODUCTION

According to *TRADOC Pamphlet 525-92*, the United States of America postulates that on the horizon in 2025 the Operating Environment/OE will face two major dilemmas or, more accurately, there will be two major factors that will determine its shape. The two key points are determined by *"the one dealing with rapid societal change spurred by breakneck advances in science and technology and the other with the art of warfare under these conditions, which will blur the differences in the art of war with the science of war"* (TRADOC Pamphlet 525-92, 2019, p. 10).

Having as a starting point the first factor, according to the same doctrine, we can add that the operating environment will be characterized by a number of elements, such as instability, with consequences that will be seen in geopolitics, the intensification of nationalism, demographic changes or competition for resources. In this enumeration, we also add that technological development will have an important contribution to make to the intensification of these issues, with their effect on human interaction and the speed of reaction to the listed issues, as well as their impact on the economic and social spheres.

The second factor determining the future operating environment will be characterized by elements such as *multi-domain operations, the conduct of operations in a much more complex terrain (urban areas), hybrid strategies, weapons of mass destruction* and *advanced (emerging and disruptive) technologies*.

NATO's perspective, whether we refer to strategic documents such as the *NATO Doctrine* or *NATO 2030 – A Strategy for a New Era*, has common elements such as circular (360°) defence, defence of the Alliance's eastern side or the development of capabilities designed to support mobility that are powerful and long-lasting. The *NATO 2022 Strategic Concept* also emphasizes that the greatest threat to the North Atlantic Alliance is posed by the Russian Federation and its subversive actions against the Euro-Atlantic area. In the same context, China is portrayed as an agent of various threats to the security stability of the Euro-Atlantic area, through mechanisms similar to those found in the case of Russia.

To highlight its role as a regional pole of power assumed also through the issued national strategies (National Defence Strategy of the Country, Military Strategy

of Romania), Romania signed the memorandum in which Türkiye and Bulgaria took part and, at the same time, it has also proposed *a safe navigation in the Black Sea* (Tîlvăr, 2024), in January 2024. This memorandum, entitled *Memorandum of Understanding on the establishment of a Task Force to Counter the Sea Mines in the Black Sea – MCM Black Sea* (Ministry of National Defence, 2024), aims, first of all, to *"demonstrate the [...] joint commitment to counter the threats of drifting mines in the Black Sea*" (Ib.), by focusing the joint effort of the three signatory parties to the memorandum.

The context presented in the introduction of this article also serves to provide an overview of the context generated by the present and future operating environment and the role that Romania plays on the eastern side of NATO, as well as to present the scientific literature that is the basis for the paper and that supports our research effort throughout the paper. In addition to the documents already listed in the previous paragraphs, there will be other works, covering the development of ideologies in the area of defence and international relations, which are meant to support our endeavour to provide a relevant and complete format to the already established research study.

Starting from the hypothesis presented in the abstract of the article, according to which "Romania is a member that is an essential contributor to NATO's defence mission in the current security environment and the existing threats to it, now and in the future", we will structure the paper in three chapters. In the first chapter, our attention will be focused on presenting the current state of the operating environment, the second chapter will be a visionary form with a focus on the operational environment of the future, and in the third chapter, we will integrate the basic ideas discussed so far to emphasize Romania's role on the eastern side of NATO in an attempt to validate the hypothesis from which we start.

In achieving this objective, we will employ research methods commonly used in social sciences, with a focus on historical analysis, document analysis, and comparative analysis, which will be key in producing relevant results in this field of study, where our approach will involve conducting descriptive research.

One of the aims of this article is to contribute to the current body of knowledge in the specialized scientific field by offering valid perspectives on Romania's NATO membership, particularly from a geopolitical and geostrategic standpoint, within both current and future operational environments.

The factors that motivated this research include the unprecedented advancement of technology, the various threats to Euro-Atlantic security, and Romania's growing

significance in the eastern side of Europe. In light of these aspects, we believe the current and future operational environments must be clearly defined in relation to the three issues, which are of interest not only to the military sphere but also to the broader scientific community.

Building on the existing state of knowledge, as outlined in the introduction, we will further explore these issues to offer a series of realistic and concise conclusions in line with the results we aim to achieve.

CURRENT OPERATING ENVIRONMENT

To provide a picture as broad as possible of the current operating environment, we will use a classification of the main factors influencing its dynamics. In this regard, we identify both major state actors and advanced, emerging, and disruptive technologies as factors that have the potential to shift the balance of power and influence the security environment.

We limit ourselves to presenting these two *factors* mentioned in the previous paragraph, because their volatility and dynamics can offer, either now or in the future, new courses of action with the capacity to bring about continuous and decisive changes in the operating environment.

The Influence of State Actors on the Current Operating Environment

The latest NATO Strategic Concept (NATO Strategic Concept, 2022), as well as the subsequent NATO summits (Vilnius – 2023, Washington – 2024), demonstrate, through their content, a solid and firm stance against the *"autocratic*" ideologies espoused by states such as North Korea, Iran, and China and, last but not least, the Russian Federation (NATO's Washington Summit, 2024), which continue to generate constant and unfounded threats to Euro-Atlantic security.

Russia is considered by the North Atlantic Alliance, according to the latest summits, to be the primary state actor generating actions that are contrary to the visions of Western countries. In this context, we highlight the conflict in Ukraine, where new actions to support Ukraine in the face of Russian aggression were reassessed during the last meeting of the member states (Smith, 2024). In this framework, the role Russia plays at the international level and how it can influence both the security and operational environments is underscored, given that a significant portion of the capabilities and capacities of NATO member states are impacted by the armed conflict in Ukraine. Thus, we can emphasize that there are

long-term effects, affecting industry, the economy, technology, and other sectors, as well as society as a whole, from a psychological perspective, especially among the current population and future generations.

Regarding the war between Russia and Ukraine, an important role is attributed to China, which, as stated in the text of the Washington summit in July 2024, is one of the states that *"helps Russia wage its war on the European continent*". To validate this statement, in May 2024, US Secretary of State, Antony Blinken, declared that *"What's not happening is the provision of actual arms by China to Russia for use in Ukraine"*, but that China is helping Russia develop the necessary technology to conduct the war waged on Ukrainian territory (Kelly Ng, Yi Ma, 2024). It is also noted that China's exports to Russia have been increasing significantly in terms of components that can be used for the construction of weapons (Sher, 2024).

The two states outlined above are joined by Iran and North Korea, as discussed at the Washington summit, which, sharing common political ideologies, are creating conditions that could destabilize the Euro-Atlantic security environment by directly or indirectly supporting the Russian-Ukrainian conflict.

Currently, the threat from the Russian Federation to the security of the North Atlantic Alliance is high, as a result of actions that produce negative effects on European states due to the fighting in Ukraine and the hybrid warfare continuously waged against Western states (Bilal, 2024). The intensification of instability is also reflected in the statements made in the public sphere by Russian officials regarding the use of nuclear weapons, along with changes in its nuclear doctrine (Richardson, 2024). Looking into the *"past"* of the war in Ukraine, specifically the fall of 2022 (Picciotto, 2024), we can see that this method of attracting the attention of the international community is repeating itself, even if it is difficult to predict how the Russian Federation will continue to pursue its interests.

The current operating environment is also characterized by the increasing number of North Atlantic Treaty Organization member states. Thus, the accession of Finland (2023) and Sweden (2024) opens new horizons for the North Atlantic Alliance. Beyond the military aspects, this territorial enlargement represents a geopolitical and geostrategic advance for NATO, while also facilitating access to the Arctic region (Gosnell, Jensen, 2024), where competition over this area is evident, with the *"bloc"* of Western and Eastern powers once again facing off against each other.

According to an article published by *Reuters* in 2022, Russia and China's interest in the Arctic region is growing, and military activity is high, with military bases

deployed in the area and military exercises conducted, even surpassing NATO's efforts (Gronholt-Pedersen, Fouche, 2022). A transposition of this framework to the main topic of this chapter suggests that, regarding the Arctic Ocean, at the time of the article's publication, NATO needed to act accordingly to keep pace with the two states involved in this region. The North Atlantic Alliance, according to the same publication, *"would need 10 years to match Russia's military presence in the Arctic"*.

When we refer to the Arctic, we must also highlight the interests of the People's Republic of China (PRC) in the Arctic. Although the United States of America does not recognize China's status as *a "Near Arctic State"* (Millard, Lackenbauer, 2021), the fact that China conducts economic activities in this region and, even in isolation, military exercises, requires that NATO's interest should be heightened. Likewise, the PRC's strategic initiative – *"One Belt, One Road*" (Department of Defense, 2019) connects China's interests with the Arctic and, at the same time, reinforces its presence in Arctic Ocean waters.

In examining the current operating environment, it is evident that, akin to the dynamics observed during the Cold War, the concept of *"state individualism"*, defined here as the capacity to act independently in domestic and foreign policy, is often *"overshadowed"* by notions of *alliance* and *partnership*. Although the dissolution of the USSR in 1991, preceded by the termination of the Warsaw Pact in the spring of the same year (Jaitner et al., 2018, p. 17), marked the conclusion of a significant chapter in human history, paving the way for new changes on the international political stage, state actors continue to identify common interests and ambitions that facilitate the formation of alliances and partnerships.

Furthermore, focusing on the eastern part of the Alliance, with Romania as a focal point, it is necessary to highlight some of the partnerships and alliances currently existing at the interstate level. The North Atlantic Treaty Organization (NATO) is regarded as the most successful military alliance (NATO, 2024) and has continued to expand its structural framework by accepting additional states, including Sweden in 2024. Moreover, the emergence of partnerships such as AUKUS (Australia, the United Kingdom, and the United States of America) and QUAD (The Quadrilateral Security Dialogue) (Panda, 2022, p. 1) indicates that states, depending on their spheres of influence and areas of interest, are forming international communities grounded in shared economic or politico-military objectives. Completing the antithetical framework between East and West, there are formalized relations such as the *"Treaty of Cooperation and Good-Neighbourliness"* between China

and Russia, as well as the *"Shanghai Cooperation Organization"*, in which Belarus, the newest member, participated in the meeting held in Kazakhstan in July 2024.

The final paragraph provides an overview of the most significant interstate relations that currently exist and contribute to the prevailing security environment. Essentially, the confrontation between states has taken on new dimensions, and, in addition to the interests dictated by military influence, the economic and political spheres are contributing to the emergence of new poles of power in the form of state organizations, as previously mentioned.

From a state-centric perspective, the current operating environment can be characterized by a condition similar to that of the post-World War II historical context, where the polarity of powers is evident, thereby generating the environment described earlier, and where its very definition can be articulated through the struggle for supremacy.

The Role of Technology in Defining the Current Operating Environment

In the publication edited by Ausubel and Sladovich – *"Technology and Environment"*, a perspective on technological rediscovery and its potential impacts on the environment is presented. Fundamentally, the end of the 1980s marks a pivotal moment in the approach of technology toward addressing environmental challenges, whether concerning coal cleaning plants or the increasing reliance on gas as a fuel source (Ausubel, Sladovich, 1989, p. 10). The growing significance of technology and technological advancements has implicitly contributed to the definition of the societal environment, which, in turn, has influenced the current security environment and the operational landscape in its present form.

A group of authors, including Elihu Zimet and Robert E. Armstrong, in a 2003 publication, offer a categorization of technological impact that encompasses five domains: informational, material, power and energy, human performance, and biological (Zimet et al., 2003, p. 2). We contend that, in reference to the current international economic, political, and military context, these elements are relevant for describing the operating environment in terms of technological evolution and its ramifications on the battlespace.

A primary area that the authors of the aforementioned study identified as crucial is information technologies. Information is indispensable in armed conflict, as in any other domain, and its impact is contingent upon factors such as *timing* and *accuracy*, which can alter the course of action at any given moment.

The National Defense Research Institute has developed a methodology aimed at ensuring the quality of information. In their work, the authors specify that through C4ISR (command, control, communications, computers, intelligence, surveillance, reconnaissance) capabilities, information will confer supremacy in military operations. Simultaneously, a rapid and high-quality flow of information is anticipated to revolutionize command and control (C2) in future battles (Ib., p. XIII). The key elements in this context are C4ISR operating systems designed for the collection and processing of data and information, enabling continuous updates on the battlefield situation. The extensive technologization to which both military and non-military spheres are currently subjected affords more advantageous levers for operationalizing the concept of *Multi-Domain Operations*.

In furtherance of the idea presented at the conclusion of the previous paragraph, we wish to draw attention to the Joint All-Domain Command and Control (JADC2, 2022) strategy of the United States of America. For this strategy to achieve its intended efficacy, ISR (intelligence, surveillance, and reconnaissance) capabilities are deemed essential, as it aims to accelerate decision-making, provide real-time battlefield situational awareness, and enhance the probability of mission success (C4ISR Through Next Generation Artificial Intelligence).

Material technologies constitute the second technological category that exerts a significant impact on the operating environment. The classification provided in the study by Elihu Zimet and Robert E. Armstrong regarding the importance of technologies identifies two types of material technologies: *functional* and *structural*. In this context, the category of functional materials encompasses electronic products, transistors, resistors, and similar items, whereas the category of structural materials includes materials characterized by properties such as corrosion resistance, strength, density, and other mechanical characteristics (Biswas, Visell, 2019).

We consider it essential to highlight this technological category in the present work because the current objective is to develop the most reliable devices for use on the battlefield. In this regard, it is pertinent to note that the drones currently being developed and deployed in the ongoing conflict in Ukraine fall within the realm of material technologies. Specifically, we will examine the latest technological innovations utilized in this conflict, without undermining the rationale of conventional warfare in this context, namely: the *"dragon drones"* (Al Jazeera Staff, 2024) and *"land-based drones"* (Robertson, 2024). The fabrication of these

technologies underscores the importance of material technologies, as well as the advanced state of current technologization. Consequently, we identify a *"volatile"* operating environment characterized by innovation and flexibility of combat assets. Furthermore, adaptation to *terrain* or *weather conditions*, and of course, in relation to the enemy's intentions and actions, occurs in near real-time through the integration of emerging and high-performance technologies.

The third category that complements the framework established by the role of technology in shaping the current operating environment encompasses the power and energy factors associated with the technical means employed by military forces. This category encompasses a range of devices that can be utilized in armed conflict situations through the enhancement of existing energy systems. Specifically, it highlights capabilities that leverage *compact, lightweight,* and *long-lasting energy sources* (Zimet et al., p. 4). In this regard, the North Atlantic Treaty Organization (NATO) issued a document in 2015, *"NATO Smart Energy*", which aimed to improve the efficiency of military structures by focusing particularly on replacing fossil fuels with renewable energy sources (NATO, 2015). Following this initiative, during the 2021 summit in Vilnius, the NATO Energy Security Centre of Excellence for Energy Security released a strategy addressing energy efficiency and *renewable energy solutions* designed to ensure the operational effectiveness of military forces during logistical operations, where energy dependence – defined in terms of fuel requirements – is dictated by geographical considerations, climate, intensity of military actions, and other factors (NATOESCE, 2021, p. 6). Thus, it is evident that the North Atlantic Alliance is actively pursuing measures to align itself, firstly, with global climate change imperatives and, secondly, to keep pace with technological advancements in the domain of independent energy sources.

In this category, we also seek to include *advanced propulsion systems for aircraft, missiles, and access to space*, the latter being recognized as one of the five accepted domains of military operations. To achieve efficiency and effectiveness with these capabilities, hypersonic propulsion for both hypersonic aircraft and hypersonic missiles is sought. In pursuit of this objective, the United States of America has initiated the development of the world's fastest airplane, the SR-72 (Gladwell, 2021). Key aspects that merit emphasis include the speed this aircraft can attain, specifically Mach 6 (equivalent to six times the speed of sound) (Moskvitch, 2010), and its operational capacity in the battlespace without the physical involvement of human personnel, as it is remotely controlled.

The topic of supplementing and securing energy needs for military operations has been examined in various scientific studies. For instance, the implementation of photovoltaic systems or hybrid solutions utilizing both solar and wind energy among NATO member states is detailed in a collective work by Mariusz Fraczek, Krzysztof Górski, and Leszek Wolaniuk (Fraczek et al., 2024). They underscore the significance of these renewable energy sources, identifying countries such as Greece, Germany, the United States of America, the United Kingdom, and the Netherlands as having initiated extensive research efforts following the *NATO Intelligent Energy* programme. It can be concluded that energy represents one of the critical factors in military operations, as evidenced by both historical and ongoing conflicts, such as the war in Ukraine. Consequently, the integration of renewable energy sources is poised to alter the landscape of the battlespace, creating new opportunities for combatants.

Today's operating environment is defined by the management of the most important *"component"* of the battlespace, *the human*, or, according to the categorization we detail in this paper, the human resource. The performance of the human factor is enhanced by technological assistance; thus, the success rate of human action in the workplace increases significantly (Bondarouk et al., 2017). In other words, in light of technological developments, individuals benefit from training through immersive *virtual training programmes* and *distributed distance learning*. For military personnel, war gaming facilitated by advanced technologies, which translates physical reality into virtual reality, helps cultivate experiences aimed at enhancing learning and/or improving skills (such as leadership and decision-making) (Checa, Bustillo, 2019, p. 12), with the objective of applying these skills in real-life situations. At the same time, this approach can also contribute to the morale of the individuals involved in the learning process. The study by David Checa and Andres Bustillo demonstrates that learning through virtual reality exposure is more effective than learning through traditional methods (Ib., p. 14).

Another aspect concerning *the individual* as a human resource is represented by the enhancement of this performance through technology. In this regard, both the level of physical resilience to various situations and the improvement of mental abilities are sought. A study conducted by James C. Spohrer and Douglas C. Engelbart analyses the influence that technologies can have on human performance. To achieve this objective, they focused on two areas – *science* and *business* – and ultimately concluded that, from a scientific perspective, technological evolution

exerts influences on five systems: *physical (atoms and molecules), biological (DNA), cognitive (the human brain), social (organizations), and technical (computers)* (Spohrer, Engelbart, 2004, p. 72). In relation to the military sphere, the current training methods, which are largely assisted by technology (GPS, virtual reality, UAS/UAV etc.), combined with the availability of various dietary supplements intended to enhance human abilities, underscore that technology finds its applicability across the five levels described by the aforementioned authors. A more extensive study in this regard could serve as the theme for a future paper analysing human performance strictly from the perspective of technological evolution, both for the present and the future.

At the end of this overview of the current operating environment, we aim to correlate with the final element of Zimet and Armstrong's classification – *biotechnologies* – a decisive component for the preparation and execution of military operations, specifically *military medicine*. It is likely that medicine will continue to be the primary application of biotechnologies for military purposes. A conclusive example in this regard is the treatment of wounds using light-emitting diodes (LEDs), which can lead to a reduction in recovery time of up to 50%, as well as the disinfection of water by destroying harmful bacteria, as demonstrated in a study published in the journal *Water Research* (Song et al., 2016). The role of biotechnology in enhancing soldiers' capabilities on the battlefield through new protective and weaponry systems is further explored in Andrew Bickford's study published in *Current Anthropology*. Here, the concept of utilizing biotechnologies to develop protective equipment capable of transmitting real-time health status information to both the individual soldier and their commander is presented (Bickford, 2019). Notably, the contribution of biotechnologies to the military sphere is much broader; however, the salient point underscores a dynamic and constantly evolving operational environment, shaped by technological advancements that reach new heights daily.

PREDICTABLE OPERATING ENVIRONMENT

In the first chapter of this article, we analysed the physiognomy of the current operating environment through a number of factors that we deemed relevant. We found that geographical location, state actors, and technological implications shape the environment in which we conduct our daily lives. One outcome of effective planning is the translation of human actions into future scenarios, whether they

pertain to short-, medium-, or long-term periods. To elucidate this preamble, we will subsequently examine scientific and specialized documents that aim to define the future operating environment and are accessible in the public domain.

To make a highly reliable forecast, it is essential to refer to the most recent events. A new outlook for the period 2024-2030, published by the US Army Training and Doctrine Command, *The Operational Environment 2024-2034*, is particularly conclusive in this regard. The report revisits the document issued in 2021, *The Operational Environment 2021-2030: Great Power Competition, Crisis, and Conflict,* which focuses on the competition with the Russian Federation and the People's Republic of China, as well as the strategies for managing the impacts of the COVID-19 pandemic.

The transformations that have occurred within the operating environment have necessitated the development of a strategy commencing in 2024. The significant issues highlighted by the United States of America include the ongoing competition with the People's Republic of China, the threats emanating from Russia's military campaign in Ukraine, as well as the challenges posed by other *"hostile"* states that jeopardize the security environment, specifically Iran, North Korea, and various extremist groups.

Building on the observations and assessments conducted by experts from *TRADOC G-2*, the USA has identified twelve conditions that possess the potential to influence military readiness and operational capability in the execution of large-scale combat operations (LSCOs) (EO 2024-2034, 2024), specifically:

- *Competition and conflict across all domains;*
- *Clustering and precision* – referring to the tendency in contemporary conflicts to prioritize mass destruction over the targeting of pre-determined objectives;
- *Proliferation of unmanned systems;*
- *Stockpiling of ammunition and weapons;*
- *Transparency on the battlefield* – attributed to the deployment of advanced technologies;
- *Increased lethality* – resulting from the use of high-precision weapons and weapons of mass destruction;
- *Anti-access and area denial (A2/AD) strategy* – a concept thoroughly examined in an article by Commander (ret.) Ion Chiorcea in *Romanian Military Thinking* (Chiorcea, 2024);

- *Logistics;*
- *Defence of national territory;*
- *Waging war in densely populated urban environments* – it is projected that by 2050, urban areas will be home to 68% of the global population (UN, 2018);
- *Information advantage;*
- *Weapons of mass destruction* – the United States of America and Ukraine assert that Russia has deployed chemical agents during military operations on Ukrainian soil (Murphy, 2024).

These *"attributes"* will guide potential military actions over the next decade, as indicated in the document published by the USA. This perspective is generally applicable to both the US military and NATO member states. Considering all the aforementioned aspects, we can anticipate a significant impact on military affairs, leading to transformations in the meaning of *military art and science, the rapid annihilation of adversaries, the dynamics of attrition warfare*, and *alterations in maneuver, fire, and defense strategies*. Furthermore, the *human resource* will increasingly be prepared to engage in combat and to lead military operations.

In contrast to the United States of America, the United Kingdom, through its *Strategic Trends Programme – Future Operating Environment 2035*, characterizes the operational environment with a slightly different emphasis while retaining the same foundational principles. Elements such as technologization, proliferation, adaptation, and nuclear weapons will play a significant role in shaping the future of military operations.

Beyond these predominantly military considerations, factors such as climate change, demographics, urbanization, and resource scarcity will also be defining for the battlespace. The balance of power is another key point for the future; although the likelihood that the United States of America will remain the largest military force by 2035 (Ministry of Defence, 2015) is substantial, the People's Republic of China is engaged in a modernization race that could elevate it to the top military position by 2050 (Hu et al., 2021). The entire described framework can be characterized as complex, dynamic, and uncertain, reflecting the *"narrow border"* that separates superpowers in their competition for economic or politico-military supremacy.

By presenting the perspectives of two key members of the North Atlantic Treaty Organization, we aim to create a general understanding of how NATO member states foresee the coming years regarding international security. To further elaborate

on the adaptability and readiness that state actors will need to demonstrate in the future, we will analyse NATO's perspective for the upcoming period. In this regard, we will substantiate the continuation of this work by outlining the notions we consider essential in the document *NATO 2030: United for a New Era*.

The North Atlantic Alliance reiterates, through this document, the importance of strengthening dialogue with China and Russia, as well as outlining methods to counter potential threats from these nations (NATO, 2022, p. 12). The perception of the risk that Russia poses to Euro-Atlantic security is also reflected in NATO doctrine (AJP-01). Practices such as *disinformation campaigns*, *cyber-attacks*, and *interference in the electoral* processes of certain states (AJP-01, 2022, p. 18) provide allies with reasons to enhance their levels of protection against such threats. Although the two superpowers mentioned above have the potential to jeopardize the security environment and may lead to new developments in the characteristics of the operating environment (political-military decisions, economic events etc.), other actors also possess the capability to create similar situations. Thus, terrorism continues to be one of the greatest destabilizers of the security environment, and its effects have not diminished within the time frame envisioned by *NATO 2030: United for a New Era*.

According to experts Pál Dunay and Matthew Rhodes, *terrorism* is identified as the most asymmetric threat to the security of citizens and to international peace and prosperity (Dunay, Rhodes, 2022, p. 9). Consequently, the threats both at present and for the foreseeable future are generated by two types of actors: state actors and non-state actors. In this respect, it is difficult to ascertain which of the two entities poses a greater degree of threat, as it depends on their methods of action. However, it can be concluded that the interests of the international community are best served by defensive measures against situations that threaten safety and security.

In NATO's vision for defining the operating environment of the future, factors such as global warming, nuclear weapons, political cohesion, and the expansion of international relations with states or organizations located south of the Tropic of Cancer are critical considerations. These potential future approaches indicate a high level of ambition on the part of the Alliance and its members to support state entities that share a common ideology, whether political, military, or economic.

The territorial scope of the North Atlantic Alliance is *"limited"* on the eastern side by states such as Poland, Romania, Bulgaria, and Türkiye. Given that the most

prominent threats originate beyond the Alliance's eastern borders (notably from Russia, Iran, and China), the aforementioned states will, in practice, represent a geostrategic and geopolitical centre of gravity for the future of the Alliance. The validation or invalidation of this assumption will be addressed in the next, and final, chapter of this paper, where we will endeavour to identify Romania's role on NATO's eastern side. This analysis will be based on national and international documents, considering the current and future security context in accordance with the information presented thus far.

THE ROLE OF THE ROMANIAN ARMED FORCES ON THE EASTERN SIDE OF THE NORTH ATLANTIC ALLIANCE

Romania's position as a member state of the North Atlantic Treaty Organization provides the advantage of being part of the most effective alliance in history (Dunay, Rhodes, 2022, p. 7). This fact can be considered a significant gain, particularly in light of the interests of major international players. However, beyond this asset, Romania faces challenges dictated, on the one hand, by its geostrategic positioning and, on the other hand, by the threats to the Euro-Atlantic space that emanate from the eastern side of the Alliance. Consequently, the Romanian state serves as the primary area of contact for many of these threats.

The role that Romania has assumed as a NATO member state will be analysed, as specified in the previous chapter, toward the end of this article, drawing on documents present in both the national and international scientific literature. In doing so, we aim to highlight key elements that will outline a framework of interest for the academic community.

According to *Romania's Military Strategy – 2021*, Romania assumes the mission of being a regional security pole and a centre of regional stability (Ministry of National Defence, 2021, pp. 10-13). This position was reiterated in 2021, particularly in relation to the characteristics of the security environment at that time. Furthermore, this assertion remains unchanged and is reinforced by the steps taken in the politico-military and economic spheres through the procurement of military technology in accordance with established programmes (Tudosia, 2024).

The war in Ukraine appears to have intensified Romania's interest in strengthening its strategic position on the eastern side of the North Atlantic Alliance. In this context, the acquisitions of various military technical items, such as PATRIOT batteries (Allied Air Command, 2024), PIRANHA V armoured vehicles

(Heiming, 2020) – in accordance with the contract for the acquisition of PIRANHA V armoured vehicles signed on 12 January 2018 (Ministry of National Defence, 2018) – and HIMARS capabilities (Defence Security Cooperation Agency, 2017), further reinforce this notion.

In the same framework, given Romania's position on the eastern side of the Alliance and within the European Union, it assumes, according to the Defence White Paper issued in 2021, the role of *a security pillar*. It is further reinforced by the fact that the Romanian Armed Forces are engaged in an extensive modernization process through the acquisition of military technology and equipment, as described in the previous paragraphs, which will have the capacity to be operational across all five operational environments. Additionally, the presence of multinational commands on Romanian territory (Headquarters Multinational Corps Southeast/HQ MNC-SE, Headquarters Multinational Division Southeast/HQ MND-SE, Headquarters Multinational Brigade Southeast/HQ MN BDE-SE, NATO Force Integration Unit/ NFIU) once again provides a picture that confirms the deterrent posture in the face of possible threats.

NATO is demonstrating its firmness in the face of the threat from Russia with *battlegroups* deployed in eight of its thirty-two member states, including Bulgaria, Estonia, Hungary, Latvia, Lithuania, Poland, Slovakia, and Romania. In order to achieve unified force management to ensure promptness and effectiveness, Romania, through the Headquarters Multinational Division Southeast (HQ MND-SE), ensures the operational capability of the four battlegroups present in Romania, Hungary, Bulgaria, and Slovakia (NATO, 2024).

The Madrid Summit in 2022, beyond highlighting the threats to global and Euro-Atlantic security, provided an opportunity for member states to endorse a new NATO Force Model (NATO, 2022). Essentially, this system is intended to replace the NATO Response Force, being a variant characterized by greater efficiency by providing a response on a larger scale and with greater intensity. Thus, this new model, according to the NATO Defence College/NDC, will comprise a NATO Allied Reaction Force/ARF (NDC, 2024) and will have a three-tiered structure. The first level of forces is intended to train one hundred thousand troops within zero to ten days once the crisis erupts; the second level of forces will train two hundred thousand troops within ten to thirty days with more complex capabilities than the troops in the first level, including for multi-domain operations; and the third level will comprise five hundred thousand troops trained within thirty to one hundred eighty days. *Figure 1* illustrates this structure.

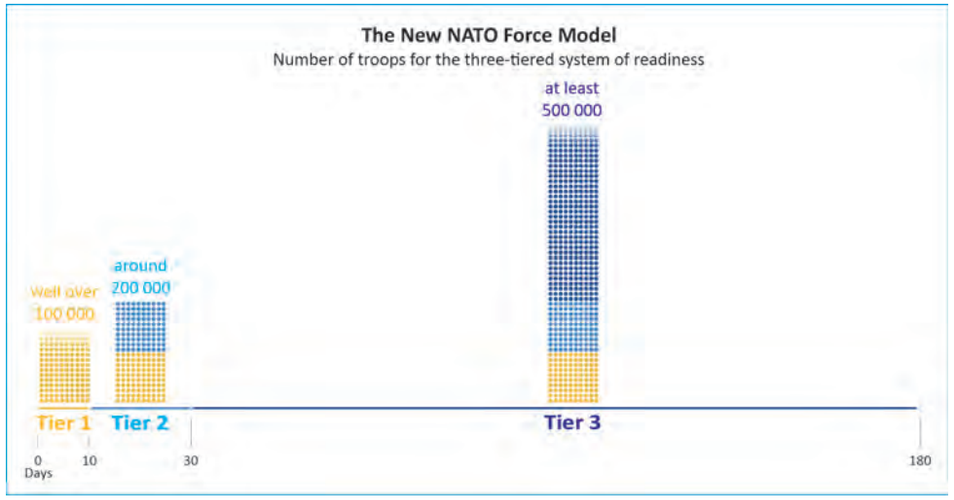


Figure 1: NATO's New Force Model (Deni, 2024, p. 3)

As the main threat is expected to come from Russia, we believe that Romania has a significant role to play, given the fact that one of the eleven army corps responsible for operationalizing the Alliance's plans and leading the allied divisions and brigades is located on its territory.

As mentioned in the introductory part of this article, Romania's position on the eastern side of the Alliance is also reinforced by the new partnership signed with Türkiye and Bulgaria concerning the establishment of a naval group in the Black Sea (Mine Counter-Measures Task Group Black Sea/MCM BLACK SEA) (President of Romania, 2024, p. 2). The establishment of this group is considered a historic milestone for this region, having strategic importance at both the regional and Euro-Atlantic levels, and it embodies the responsibility assumed by Romania and Bulgaria, given the low level of capabilities to combat sea mines compared to Türkiye, which possesses superior resources in this respect.

The outbreak of the war in Ukraine has brought Romania to the forefront by activating advanced defence plans and deploying the *Very High Readiness Joint Task Force* (VJTF) within the *NATO Response Force* to the country, followed, as mentioned earlier, by the establishment of a French-led battle group (Iacob, 2024, p. 12).

The time period covered by the new strategies on security and defence, present at the national level, will reach its limit toward the end of this year. It will entail new documents that will be adapted to the physiognomy of the current operating environment and will have to respond to new threats to national security.

Most likely, Romania will pursue its interests as a member of the North Atlantic Alliance, reiterating the objectives and missions set out in the current strategies and, at the same time, engaging in the fulfilment of missions to defend the common interests of the 32 NATO member states.

CONCLUSIONS

The dynamism of the security environment requires state actors to ensure that they take measures to increase their degree of safety against possible threats to their security. The transition from the Cold War bipolarity to today's multipolarity reflects both the military and economic development of some states and an unpredictable struggle for supremacy.

We believe that, by analysing the themes we set ourselves at the beginning of this article, we have validated the main hypothesis, namely that Romania is an essential member of the North Atlantic Alliance in the eastern part of the European continent. Romania's position as a pole of regional security and power is confirmed by the acquisition of military technology with high operational capabilities for the current and future operating environment. Also, the conclusion of new strategic-level partnerships with applicability, in particular, in the Black Sea region and the eastern region of the Alliance further reinforces the hypothesis from which we started.

In terms of the approach we have taken with regard to providing an outlook on the future operating environment, we can only assess it as a realistic one, as we have tried to follow the views from the perspective of key actors in the international security environment, as well as from the perspective of the North Atlantic Alliance. The conclusion on this issue is rendered by the instability of the security environment, with the future outlook being one that entails a high degree of uncertainty, mainly considering the massive technologization as well as the changes brought about by natural causes (climate change, demographic change etc.). To this end, states will certainly take the necessary measures to prepare themselves; thus, the desire to replace, as much as possible, human resources with artificial intelligence represents a turning point in the war of the future.

Also, through the research effort of this paper, we have aimed to highlight some of the factors that define the current operating environment. Thus, after analysing specialized and scholarly documents, we have concluded that the major state actors, as well as the fulminant evolution of technologies with emerging and disruptive qualities, are determining the current structure of society and, implicitly, of the battlespace.

We consider the classification of technological factors impacting the military sphere to be generally valid in relation to the temporal axis (past, present, and future), and the results of the research have reinforced this assumption, which, even if it did not capture the full complexity of defining elements, we believe is sufficient to support the idea from which we started. For the years to come, technologization will most likely develop even further, bringing under its spectrum a wide range of innovative components.

Finally, we express our aspiration that this article will add something new to the academic scientific environment, which would be the most valuable appreciation we modestly expect.

BIBLIOGRAPHY:

1. Allied Air Command (2024). *Romanian PATRIOT battery demonstrates readiness and operational capabilities*, 2024, https://ac.nato.int/archive/2024/romanian-patriot-battery-demonstrates-readiness-and-operational-capabilities, retrieved on 15 September 2024.
2. Al Jazeera Staff (2024). *What are 'dragon drones', Ukraine's latest weapon against Russia?*, https://www.aljazeera.com/news/2024/9/9/what-are-dragon-drones-ukraines-latest-weapon-against-russia, retrieved on 3 September 2024.
3. Arsalan, B. (2024). *Russia's hybrid war against the Wes*t, https://www.nato.int/docu/review/articles/2024/04/26/russias-hybrid-war-against-the-west/index.html, retrieved on 31 August 2024.
4. Ausubel, J.H., Sladovich, H.E. (1989). *Technology and environment*. Washington D.C.: National Academy Press
5. Bickford, A. (2019). *"Kill-Proofing" the Soldier Environmental Threats, Anticipation, and US Military Biomedical Armor Programs* in *Current Anthropology*, vol. 60.
6. Biswas, S., Visell, Y. (2019). *Emerging Material Technologies for Haptics*, in *Advanced materials technologies*, vol. 4, no. 4, California.
7. Bondarouk, T., Parry, E., Furtmueller, E. (2016). *Electronic HRM: four decades of research on adoption and consequences*, in *The International Journal of Human Resource Management*.
8. Chiorcea, I. (2024). *Conceptul A2/AD (Anti Access/Area Denial) – între teorie și practică,* in *Gândirea militară românească*, no. 1. București: Defence Staff.
9. Defence Security Cooperation Agency (2017). *Romania – High Mobility Artillery Rocket Systems (HIMARS) and Related Support and Equipment*, https://www.dsca.mil/press-media/major-arms-sales/romania-high-mobility-artillery-rocket-systems-himars-and-related , retrieved on 15 September 2024.
10. Department of Defense (2019). *Arctic Strategy*, Office of the Under Secretary of Defense for Policy.

11. Dunay, P., Rhodes, M. (2022). *The challenges ahead NATO prepares for the 2030s and beyond*, in *Concordiam Journal of European Security and Defense Issues*, vol. 12, no. 2.
12. Foggo, J.G., Fritz, A. (2018). *NATO and the Challenge in the North Atlantic and the Arctic*, in *Whitehall Papers*. Routledge.
13. Gladwel, D. (2021). *SR-72 – The US Is Building the Fastest Aircraft in the World*, https://sofrep.com/news/sr-72-the-u-s-is-building-the-fastest-aircraft-in-the-world/, retrieved on 5 September 2024.
14. Gosnell. R., Jensen, B. (10 July 2024). *NATO and the Arctic*, https://www.csis.org/analysis/nato-and-arctic, retrieved on 30 August 2024.
15. Gronholt-Pedersen, J., Fouche, G. (2022). *Dark Arctic – NATO allies wake up to Russian supremacy in the region*, https://www.reuters.com/graphics/ARCTIC-SECURITY/zgvobmblrpd/, retrieved on 31 August 2024.
16. Hu, A., Yan, Y., Tang, X., Shenglong, L. (2021). 2*050 China: Becoming a Great Modern Socialist Country*. Singapore: Springer.
17. Iacob, D.D. (2024). *Romania and the Romanian Armed Forces: 20 years in NATO*, in *Romanian Military Thinking*, no. 1. București: Defence Staff.
18. Jaitner, F., Olteanu, T., Spöri, T. (2018). *Crises in the Post-Soviet Space*, Routledge, Vienna.
19. Kaushal, S., Byrne, J., Byrne, J., Pili, G.&Somerville, G. (2022). *The Balance of Power Between Russia and NATO*, in *The Arctic and High North*. Routledge, Philadelphia.
20. Ministry of National Defence (2021). *Strategia Militară a României – 2021,* București.
21. Ministry of National Defence (2024). Memorandumul de Înțelegere privind constituirea grupului operativ pentru combaterea minelor marine în Marea Neagră – MCM Black Sea.
22. Moskvitch, K. (2010). *Hypersonic jet Waverider eyes Mach 6*, https://www.bbc.com/news/technology-19257769, retrieved on 5 September 2024.
23. Murphy, M. (2024). *Russia using chemical choking agents in Ukraine,* https://www.bbc.com/news/world-europe-68941220, retrieved on 8 September 2024.
24. NATOESCE (2021). *Energy efficiency and renewable energy solutions in NATO and PfP countries' military operations*, Vilnius.
25. NATO (2022). *Allied Joint Doctrine*, F Edition, Version 1.
26. NATO (2022). *NATO 2030: United for a new era*.
27. NATO. *NATO at 75: A Legacy of Unity and Transformation*, https://www.act.nato.int/article/nato-75-legacy-unity-transformation/, retrieved on 1 September 2024.
28. NATO (2024). *NATO's military presence in the east of the Alliance*, https://www.nato.int/cps/en/natohq/topics_136388.htm, retrieved on 16 September 2024.
29. NATO (2015). *NATO Smart Energy Capable Logistician,* https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_08/20170808_Smart-Energy-Ex-Capable-Logisti.pdf, retrieved on 5 September 2024.

30. NATO (2022). *New NATO Model Force,* https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/220629-infographic-new-nato-force-model.pdf, retrieved on 16 September 2024.
31. NDC (2024). *The new NATO Force Model: ready for launch?*, https://www.ndc.nato.int/news/news.php?icode=1937&lang=en, retrieved on 16 September 2024.
32. Ng, K., Ma, Y. (2024). *How is China supporting Russia after it was sanctioned for Ukraine war?*, https://www.bbc.com/news/60571253, retrieved on 30 August 2024.
33. Panda, J., Gunasekara-Rockwell, E. (2022), *Quad Plus and Indo-Pacific*, Routledge, London.
34. Picciotto, R. (2024). *CIA director saw 'genuine risk' of Russia using tactical nuclear weapons early in Ukraine war*, https://www.cnbc.com/2024/09/07/cia-director-russia-ukraine-war-nuclear-weapon-risk.html, retrieved on 1 September 2024.
35. Richardson, J. (2024). *Is Russia's changing nuclear doctrine a significant concern – or just another empty threat?*, https://theconversation.com/is-russias-changing-nuclear-doctrine-a-significant-concern-or-just-another-empty-threat-238078, retrieved on 1 September 2024.
36. Robertson, N. (2024). *Ukraine industry chief sees bumper year for land-based drones*, https://www.defensenews.com/global/europe/2024/07/09/ukraine-industry-chief-sees-bumper-year-for-land-based-drones/, retrieved on 3 September 2024.
37. SambaNova, *C4ISR Through Next Generation Artificial Intelligence*, https://sambanova.ai/hubfs/23945802/downloads/Product%20Collateral/SambaNova_ISR-Solution-Brief_4-7-22.pdf, retrieved on 3 September 2024.
38. Sher, N. (2024). *Behind the Scenes: China's Increasing Role in Russia's Defense Industry*, https://carnegieendowment.org/russia-eurasia/politika/2024/05/behind-the-scenes-chinas-increasing-role-in-russias-defense-industry?lang=en, retrieved on 30 August 2024.
39. Smith, S. (2024), *NATO leaders advance Ukraine's cause at Washington summit*, https://www.chathamhouse.org/2024/07/nato-leaders-advance-ukraines-cause-washington-summit, retrieved on 30 August 2024.
40. Song, K., Mohseni, M., Taghipour, F. (2016). *Application of ultraviolet light emitting diodes (UV-LEDs) for water disinfection: A review.* Water Research, vol. 94.
41. Spohrer, J.C., Douglas, C.E. (2004). *Converging technologies for enhancing human – Science and business perspectives,* in *Coevolution of human potential and converging technologies*, vol. 1013. Los Angeles.
42. Tîlvăr, A., in Ministry of National Defence, 2024, see source no. 21.
43. 43. TRADOC Pamphlet 525-92 (2019), Army.mil, https://adminpubs.tradoc.army.mil›pamphlets, pdf., retrieved on 22 May 2024.
44. TRADOC G-2 (2021). *The Operational Environment (2021-2030): Great Power Competition, Crisis, and Conflict.*
45. TRADOC G-2 (30 July 2024). *Operational Environment 2024-2034: Large-Scale Combat Operations*.

46. *Treaty of Good-Neighborliness and Friendly Cooperation Between the People's Republic of China and the Russian Federation* (2001), https://www.peaceagreements.org/viewmasterdocument/1735, retrieved on 2 September 2024.
47. Tudosia, M. (2024). *Romanian acquisition programmes: a steady path to reindustrialisation*, https://euro-sd.com/2024/05/articles/38168/romanian-acquisition-programmes-a-steady-path-to-reindustrialisation/, retrieved on 15 September 2024.
48. United Nations (2018). *68% of the world population projected to live in urban areas by 2050*, https://www.un.org/development/desa/en/news/population/2018-revision-of-world-urbanization-prospects.html, retrieved on 8 September 2024.
49. Zimet, E., Armstrong, R.E., Donald, C.D., Mait, J.N. (2003). *Technology, Transformation, and New Operational Concepts*. Defense Horizons. Center for Technology and National Security Policy, National Defense University.

THEORETICAL-PRACTICAL INCONGRUENCES OF LOGISTIC SUPPORT IN THE FIGHT FOR THE CONQUEST OF KYIV

Major Superior Instructor Ana-Maria MERLUȘCĂ, PhD Candidate
"Carol I" National Defence University, Bucharest
Colonel Professor Cristian-Octavian STANCIU, PhD
"Carol I" National Defence University, Bucharest
DOI: 10.55535/RMT.2024.4.04

In the initial stage of the invasion of Ukraine, logistic support for Russian forces faced major difficulties. Although the Russian Armed Forces' logistic doctrine outlines a robust capacity to support forces, in practice, poor execution of logistic support led to operational failures. In this article, we will highlight the aspects that contributed to Russia's inability to logistically support its own forces in the fight for the conquest of Kyiv. Thus, we will examine theoretical elements regarding the conception and organization of material-technical support structures and will detail practical aspects observed in the execution of logistic support for Russian troops. The purpose of the article is to highlight the discrepancies between the theoretical aspects and the execution of logistic support for the Russian forces that fought in the battle for Kyiv. The authors aim to justify that planning and logistic estimates during the battle for Kyiv did not adhere to relevant doctrinal directions, which contributed to military failures. As for the employed research method, we opted for content analysis of data extracted from military specialties books, doctrines, and publications in the field of military sciences, as well as from the NATO collection of lessons identified on the Russian-Ukrainian front.

Keywords: logistic support; Russian forces; battle for Kyiv; doctrine; military science;

INTRODUCTION

In this endeavour, we aim to highlight theoretical aspects of logistic support in offensive operations. The unsuccessful application of the mentioned aspects by the Russian armed forces contributed to the failure of the battle for Kyiv, with incalculable losses even at this moment. We started from the observed state of affairs in the theoretical space of Russian military logistics, from which we determined that planning and logistic estimates during the battle for Kyiv did not adhere to relevant doctrinal directions.

To support our exposition, we analysed doctrinal elements of the logistic conception of the Russian Federation's armed forces and related them to the organization of logistic support forces and the specific activities carried out, to the conception of material provision for the forces, and to logistic support for expeditionary operations.

In practice, it has been demonstrated that the current Russian military logistic system is neither organized, trained, nor equipped to provide the expeditionary logistics necessary for operational success. The main dilemmas faced by the Russian armed forces were significant logistical problems, including difficulties in road and rail supply. While some authors (Martin et al., 2023) argue that the failure to achieve the objective of conquering Kyiv by the Russian armed forces was largely caused by poor planning by Russian logistician's support for the operation, other specialists believe that military failure led to the inability to achieve proper logistic support (Skoglund et al., 2022). Regardless of the position we take, one fact is certain: the execution of logistic support for Russian troops in the battle for Kyiv faced incalculable difficulties.

The consequences of the execution of the plan to occupy Kyiv in 2022 demonstrated the application by the Russians of a deficient strategy, especially for achieving logistic support. In the initial stage of Russia's offensive operation, the repercussions were clear: military convoys were ambushed, essential military equipment (such as battle tanks) broke down or ran out of fuel, insufficient combat rations, illnesses, and frostbite among soldiers (Berkowitz, Galocha, 2022).

THE CONTEXT OF THE BATTLE FOR KYIV FROM A LOGISTIC PERSPECTIVE

In the spring of 2022, the entire world witnessed the significant losses of the Russian armed forces in the battle for Kyiv and the success, which was very hard to anticipate in February 2022, of the actions of the Ukrainian armed forces. 24 February 2022 marked the initiation by the Russian Federation of a special operation in Ukraine, aiming to quickly and decisively occupy the capital, Kyiv, and to change the current government. The ground troops of the Russian Federation began the attack on Kyiv along two directions. The first direction, approximately 150 km long, was the Belarus-Kyiv axis, where forces equivalent to four regiments, with about 15,000-20,000 soldiers each, were deployed (Nistorescu, 2022, p. 133). The second offensive direction involved forces at the level of two divisions, deployed from the Chernihiv and Sumy regions toward the capital of Ukraine (Vershinin, 2022).

Most likely, Russian strategists planned the operation based on the assumption that the capital of Ukraine would be conquered within three days. Contrary to Russian plans, the achievement of the objective to occupy Kyiv and overthrow President Zelensky's government was blocked by the resistance of the Ukrainian armed forces. Numerous analyses and lessons drawn by military specialists address the causes of the operational failure of the Russians. Among the most commonly cited arguments, the logistical failure is predominant.

Challenges became evident with the identification of the supply needs of the assault troops for fuel, ammunition, and spare parts for damaged equipment. Logistic support forces failed to supply the assault troops with materials, mainly due to prolonged communication lines and lack of access to the railway infrastructure, which is vital for ensuring material supplies (Jones, 2022, p. 1). Furthermore, supply convoys of the Russian troops fell into ambushes organized by the Ukrainian forces, as the security of the rear area for the assault forces was not established. The effort on logistics was compounded by the needs for artillery ammunition, as fire support for the operation was only minimally provided by aviation.

It can be stated, almost with certainty, that planning an offensive operation along multiple axes over a front that stretches for over a thousand kilometres would inherently cause significant stress for the armed forces of any current major power, even in theory. In practice, an attack along multiple directions was heavily impacted by the inability of the Russian military logistic system to support the operational execution of the offensive plan against Kyiv. The failure to achieve logistic support is evident, as evidenced by the roadblock involving logistic vehicles. Over a length

of 70 km, military logistic columns became stuck on the only road north of Kyiv, with the assault troops no longer able to be resupplied with food and essential equipment.

The uninterrupted functioning of supply chains is fundamental for military logistics, whether in military or civilian contexts. Providing combat forces with goods such as ammunition, fuel, food, and spare parts for damaged equipment as quickly as possible can dictate the outcome of an operation, as some authors opine it happened with the Russian forces in the battle for Kyiv (Martin et al., 2023). The consequences of supply chain dysfunctionality are difficult to measure, but they certainly impact how military operations, or even civilian society, function. In fact, if we can draw a conclusion from the COVID-19 pandemic and the pressure on supply chains due to this crisis (Helper, Soltas, 2021) or from the lessons observed in the Russo-Ukrainian conflict, we could say that the uninterrupted operation of logistics systems is essential for the efficiency of today's society. Certainly, these crisis situations have affected how decision-makers within governments, armies, and industries relate to vulnerabilities in supply chains. A clear demonstration of the importance of functional supply chains emerged as early as the first months of the Russo-Ukrainian war (Cunningham, 2023, p. 2).

According to analysts, the Russian armed forces faced considerable logistical challenges, mainly due to inadequate preparation and planning of logistics, as the logistical estimates were made incorrectly, despite the Russian forces having both doctrinal support and technical capabilities.

THEORIES OF LOGISTIC SUPPORT

It can be almost accurately assumed that the initial political objectives of Russia in February 2022 were the capture of Kyiv, the collapse of the current Ukrainian government, and the annexation of certain Ukrainian territories to the Russian Federation. However, the strategy that was supposed to achieve these objectives was not only flawed but also poorly implemented. We will further refer to significant theoretical aspects for planning and estimating the logistic support needs of the armed forces in military operations.

One of the lacking factors was the execution of logistic support from the Russian armed forces, which had been absent since the initial phase of the conflict and even during the unfolding of the operation. One aspect that seems not to have been given enough consideration is the **principle of logistic sufficiency**. According to this principle, the levels and distribution of logistic resources must be sufficient to reach the necessary levels for the readiness, sustainability, and mobility

of the forces. Moreover, Russian military strategists did not accurately appreciate the requirements to which the national defence infrastructure had to respond, and it was overwhelmed not only by operational demands but also by the effects of the economic sanctions imposed by the European Union countries. In addition, the motivation of the Ukrainians to defend their existence as a state and the high degree of resilience demonstrated were factors that caught Russian planners by surprise, especially in the field of logistics (Ti, Kinsey, 2023, p. 383).

Military experts agree that the Russian armed forces were sized to demonstrate rapid and overwhelming fighting power. However, it is clear that the failure of the operation, at least in the initial months, was due to weaknesses in the Russian logistic system. We can assert, almost with certainty, that Russian military strategists did not expect the response from the Ukrainian armed forces, but rather had in mind a quick and categorical victory. Michael Kofman, the director of the program for Russian studies at the Center for Naval Analyses (CNA) in Virginia, USA, opined in March 2022 that: "*We can suspect* [that Russians] *did not properly organize the logistics necessary for an effective Plan B, which was to have an actual, serious fight in what is the largest country in Europe outside of Russia"* (Berkowitz, Galocha, 2022).

In this paradigm, the war in Ukraine can be classified as a *"conflict between hopelessly unequal forces"*, following the **model of international conflict** proposed by Boulding (1988, p. 244). The American economist classifies potential participants in a conflict into six types: 1) tribe, 2) feudal or agricultural society, 3) universal agricultural society, 4) industrial power, 5) superpower, 6) world state (global). He envisions three categories of international conflict in which the previously mentioned powers can be engaged: (A) conflict between equals, (B) conflict between unequals, and (C) conflict between hopelessly unequal forces. Although the war between Ukraine and Russia appears to have begun under the auspices of category (C), it nonetheless shows a change in its character, opposed to the reasoning of conventional international conflicts. To draw a simplified analogy, we can state that Ukraine fits into Boulding's theory as an agricultural society. Since February 2022, this state has found itself involved in a conflict with a superpower, the Russian Federation. Thus, we can observe that the nature of the Russo-Ukrainian conflict adheres to the category of conflicts between hopelessly unequal forces. The inequitable conditions of hostilities during the initial phase of the Russian invasion were balanced by factors we intend to detail further. The first factor refers to the possibilities of logistic support for the Russian armed forces expeditionary operations. The second factor we will elaborate on is the requirement to adapt

the Russian armed forces logistic doctrine to the offensive operation in Ukraine, with an emphasis on the battle for Kyiv (Boulding, p. 245).

Organization of the Logistic Support Structures of the Russian Forces

For a clearer understanding of the logistic support actions of Russian forces, we consider it necessary to examine some doctrinal elements of the **logistic conception in the Russian Federation's armed forces**. We will refer to the organization of logistic support forces and the specific activities carried out, the conception of ensuring materials for the forces, and the logistic support for expeditionary operations.

The term used for the structure executing logistic support in the Russian armed forces is the **Material-Technical Support Structure** *(Materialno-tekhnicheskogo obespechenie)*, and we will continue to use the acronym MTO (Milevski, 2022, p. 3) to refer to these organic logistic support structures. Russian armed forces logistics, despite its differing nomenclature from that of Western armed forces, adheres to the same logistic principles and performs the same specific functions necessary to mobilize troops and provide them with all the essential materials for conducting military actions. Organizationally, the echelons subordinate to a brigade do not possess independent material-technical support structures, and specialized support is provided through organic structures (platoon or company). Thus, combat structures up to the brigade level are supported by elements belonging organically to the unit or received as support, to ensure the troops have supplies and to carry out maintenance of equipment. As Grau and Bartles note, within the ground forces, regiments are logistically supported by a company MTO, manoeuvre brigades have a battalion or a company MTO in their composition (depending on the type of brigade), and divisions are supported by a battalion MTO. At the level of the combined arms army (CAA), a MTO brigade operates, managing supply depots (Grau, Bartles, 2016, p. 322).

We can observe that the **specific activities of the material-technical support structures** (Ib.) have a certain correspondence in the logistics of the Romanian Armed Forces:

- providing armed forces with weapons and military equipment;
- supplying fuel and materials (uniforms, equipment, inventory and maintenance goods etc.);
- feeding and equipping personnel;
- ensuring the facilities necessary for washing and repairing clothes;
- repairing and restoring the functionality of roads and railways;
- organizing the transport of personnel and materials;
- receiving, managing, and distributing materials from depots;

- organizing preventive maintenance and repair of weapons, military equipment, and materials;
- ensuring maintenance and repair services for buildings and public utilities in military installations;
- carrying out calibration activities in the field of metrology;
- training military personnel from other specialties regarding the execution of specific material-technical support activities;
- conducting controls related to feeding and fire protection in military installations (*Romanian Armed Forces Joint Logistics Doctrine*, 2023, p. 28).

According to the organizational and personnel structure, mobile and stationary forces and facilities are included in the MTO system of the military district to which they belong. The basis of the mobile component consists of permanent logistic teams with a high level of response, while the foundation of the stationary component consists of complex storage bases that contain all the necessary stock quantities of material and technical means. According to statements by Major General Andrey Bulyga, the logistics deputy commander of the Central Military District (Vershinin, 2022), the main task of the MTO is to maintain the combat readiness and combat capability of the troops through the effective use of military command and control organs, forces and assets of the MTO.

The logistical concept of the Russian armed forces stipulates that the MTO brigade sends supplies from warehouses to the MTO battalions that support the manoeuvre brigades of the army groupings and to the artillery groupings of the brigade, as represented in *figure 1*.

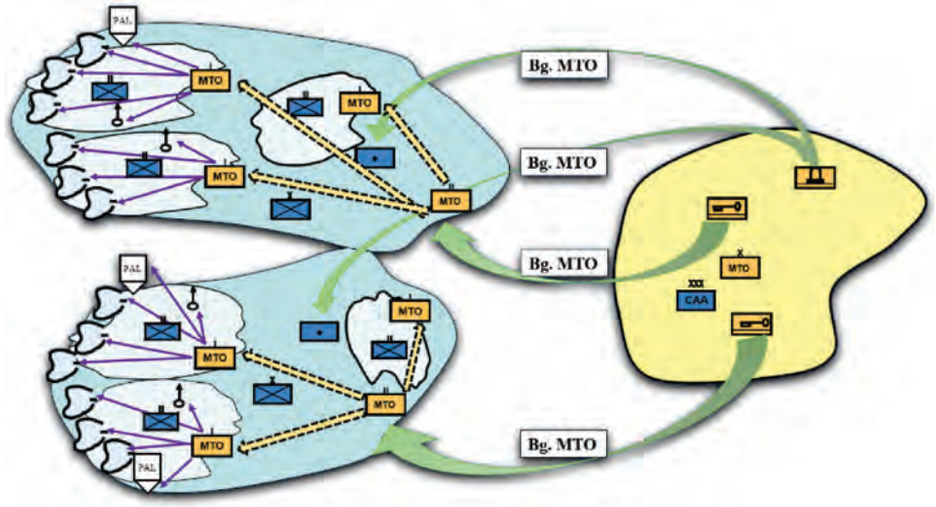


Figure 1: The flow of material supply to the Russian forces (authors' design)

The MTO battalions are to push materials to the MTO companies and, as applicable, to the mortar batteries. The MTO companies supporting the manoeuvre battalions will resupply combat units and combat supply points. If the MTO structures cannot push all necessary supply materials forward, their effort will be supplemented by the MTO battalion (Martin et al., 2023, p. 3).

Logistical Support for Expeditionary Operations

A definition of expeditionary operations can be simplified by the capability to project military power over extended lines of communication in a distant operational area to achieve a clearly specified objective (*Joint Operations, Joint Publication 3-0*, 2017, p. 213). Clearly, by their nature, expeditionary operations are offensive since few situations can conceive of a defensive operation requiring the deployment of troops over long distances. In this paradigm, the invasion of Ukraine demonstrates a classic case of expeditionary operation requiring adequate logistical capabilities (Ti, Kinsey, 2023), particularly for robust resupply of troops over long distances.

In fact, the lengths of supply lines, according to viability theory, constitute a critical factor for conducting expeditionary military operations. Boulding demonstrates that the distance from the garrison where an armed force operates is inversely proportional to the combat capability of the force. This fact means that mobilizing forces over long distances manifests direct effects on both resupply capacity and the morale of exhausted troops. He also shows that long deployment distances imply extended supply lines that require additional protection, and thus, the combat capacity of the troops is consumed in meeting the need for security of communication lines (Boulding, p. 230).

Moreover, to support a large-scale operation over a prolonged period, particularly in an enemy territory conflict, Russian forces must rely on the railway system according to their own doctrine. In fact, with respect to force projection, perhaps the most valuable logistical capability in the Russian toolkit is the vast national railway system. The civil and military transport system largely relies on the railway infrastructure, being the primary means of providing logistical support for most military operations. Due to the importance of railways for military operations, the Russian Federation has established a separate branch, the Railway Troops, intended for the protection, servicing, and maintenance of the railway service for its armed forces. The military railway service consists of ten brigades and several independent battalions dispersed throughout Russia, operationally attached to the respective military districts. These units provide logistical support related to railway transport for military operations, including repairs, bridge construction, and camouflage (Grau, Bartles, p. 327).

Loss-of-Strength Gradient

According to viability theory, Boulding describes the conditions under which a state (or other conflict actor) can dominate another state. The theory, rooted in economics, states the conditions under which an entity has the capacity and motivation to dominate or control another entity (state, military force, commercial firm etc.). Subsequently, Boulding proposes a **model of the loss-of-strength gradient** for two opposing forces with different combat capability proportions. Specifically, the model asserts that an armed force reduces its combat capability as it moves away from the base location, and the sphere of influence (the area where the force is dominant) shrinks until the combat capability is equal to that of the opponent (point D in *figure 2*). Moreover, the costs related to the transport of troops and supplies will increase exponentially with the distance of deployment.

In this situation, we can discuss two states (A and B) that have their headquarters or general command at points A and B, respectively. The distance between the two bases is represented by segment AB. *Figure 2* reflects a representation of the model of the loss-of-strength gradient and the spheres of influence of the armed forces, according to the authors' conception.

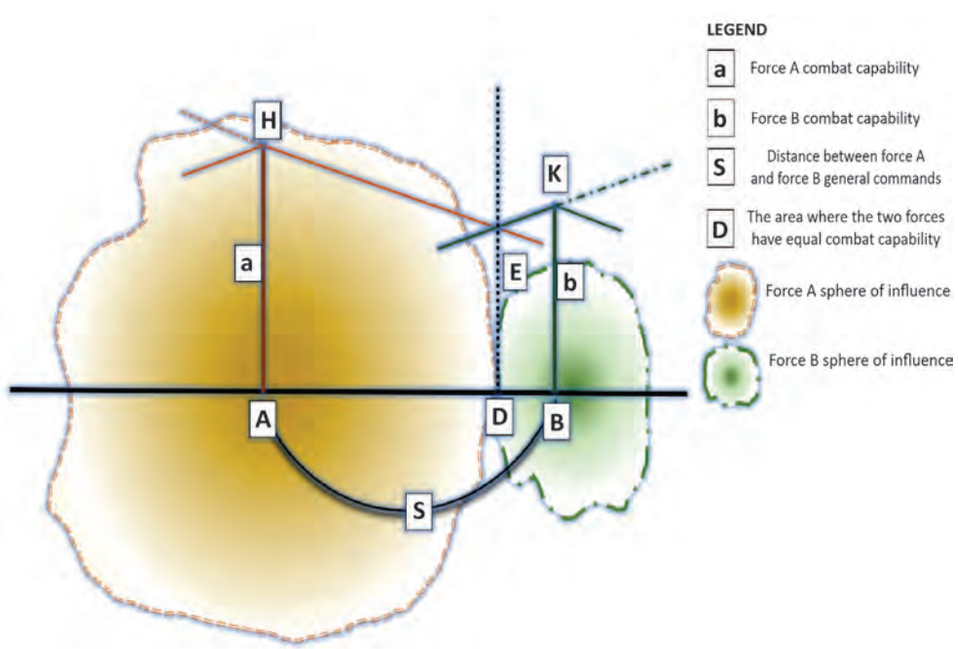


Figure 2: Spheres of influence and the gradient of combat capability loss, according to theory (authors' design)

Next, we will address the combat capability of each force, noting that the base garrison records a maximum level of combat capability (AH=a, BK=b). For a clear understanding of the term, we define combat capability as *"the state of a force at a given moment, a combination of moral, physical, and conceptual aspects [...], the result of the force generation process – doctrine, training and evaluation, equipment, morale, and other factors"* (*F.T.-1, Doctrine for Ground Forces Operations*, 2017, p. III–12). Since measuring this variable is especially difficult, only quantifiable elements such as personnel staffing, equipment, and supplies could be considered.

It can be observed that, as the distance between the base garrison and the deployment point of the forces increases, two phenomena occur simultaneously. The first phenomenon relates to the decrease in combat capability as the distance from the garrison grows, and the supply lines extend. The second phenomenon registers an increase in transport costs, directly proportional to the distance of deployment.

Referring to the first phenomenon, viability theory addresses the loss-of-strength gradient concerning the distance from the point of origin, in our case, the general command of the opposing forces. The reasoning behind the theory admits that a military force becomes weaker as it moves away from the originating garrison for several reasons, including the extension of resupply and evacuation routes, decreased efficiency of logistical support, and diminished morale of the troops.

To summarize the mentioned theoretical aspects, we can emphasize that in Russian military doctrine, the logistical concept provides the necessary capabilities to support the armed forces, theories from the field of economics highlight the importance of material supply for expeditionary operations, and the military transport system heavily relies on the railway network.

EXECUTION OF LOGISTICAL SUPPORT FOR RUSSIAN TROOPS

If we draw an analogy between Boulding's theories and the invasion of Ukraine on 24 February 2022, we can observe that the effect of distance on logistical efficiency remains relevant. As previously mentioned, expeditionary operations require robust logistics to compensate for the drawbacks imposed by extended lines of communication. However, in practice, it has been demonstrated that the current Russian military logistical system is not organized, trained, or equipped to provide the necessary expeditionary logistics for operational success.

A series of errors led to the inefficiency of logistical support for Russian troops. At the operational level, planners believed that a rapid attack with minimal material losses would lead to territorial gains without imposing the need for resupply.

Furthermore, to achieve the element of surprise, Russian decision-makers kept the troop deployment plan secret, including from logistics planners. According to studies published by military research institutes, Moscow likely expected Kyiv to capitulate within three days (Watling, Reynolds, 2022). It was the basis for the decision that combat forces would carry supplies for only five days of fighting, as stipulated by Russian armed forces logistics doctrine. As is known, Russian troops withdrew from near Kyiv by 2 April 2022, with enormous losses.

Various centres and research institutes have studied the causes of logistical failure in the battle for Kyiv. The study on *"The Failures of Russian Logistical Support in the Ukraine Conflict"* is relevant as it clarifies the causes of the disruption of logistical support for Russian forces in the initial weeks of the operation conducted in Ukraine (Martin, Barnett, McCarthy, 2023). Logistics convoys loaded with necessary materials to resupply Russian armed forces were blocked by actions of the Ukrainian armed forces.

The causes that led to dysfunctions in logistical support were numerous: the extensive size of communication lines, the use of unsecured communication networks, the destruction of bridges and railways, and the preference for artillery support over air support.

The communication lines became excessively extended due to the increased pace of the assault forces. Russian assault forces, which did not encounter significant resistance from Ukrainian defenders, successfully exploited the element of surprise. These forces advanced near Kyiv, making the resupply of ammunition and fuel the main issue for logistics planners. According to the doctrine of the Armed Forces of the Russian Federation, the logistics support brigade (MTO is the Russian acronym for this brigade) does not possess sufficient transport capability to meet logistical requirements at distances greater than 160 kilometres from railway supply sources (Hugos, Salo, Kuhns, Hazen, 2022).

The communication lines used to transmit orders or requests for logistical support were not secured. It worked to the advantage of Ukrainian forces, who were able to intercept conversations and identify the positions of Russian forces, as well as the routes of the convoys. Logistics convoys became targets for Ukrainian attacks, resulting in human and material losses. Thus, Russian resupply lines were disrupted.

Another factor contributing to failures in logistics planning was the use of unsecured communication networks for transmitting logistical orders. The assault forces acted swiftly, and the rapid pace of the offensive operation made it impossible to maintain radio connections. Therefore, communication of orders was conducted

through devices that were easily intercepted by Ukrainian soldiers. As a result, the Russian supply chain was interrupted due to Ukrainian attacks on logistics convoys. The destruction of bridges and railways (Ti, Kinsey, 2023), as well as the selective flooding of the terrain, hindered transportation efforts (Spencer, Collins, 2022). In this case, Ukrainian forces applied a lesson learned from the Second Battle of Fallujah in 2004 (Ib.). At that time, the US troops were surprised by flooding caused by a destroyed dam, and the force commander had to change the essential mission to reduce the flooding. In Ukraine's case, knowledge of urban infrastructure was crucial for the success of the adopted tactics.

Fire support was provided more by ground artillery than by air support. Since the Russian armed forces did not have the capability to achieve air superiority, and due to the lack of training of aviation pilots, air support during the battle for Kyiv was minimized. Thus, the main effort for fire support fell to ground artillery, which further burdened the logistics effort in resupplying artillery ammunition.

One reason for the poor performance of the Russian armed forces during the invasion of Ukraine was the unsatisfactory supply of material items and the low level of logistical support for Russian troops. There were numerous instances of interruptions in the operation of Russian military equipment due to a lack of fuel and ammunition, leaving personnel without food and heating. The result of such poor logistical support was low morale among soldiers and their inability to fulfil assigned combat tasks during engagements with Ukrainian forces.

In summary, we can conclude that the logistical support forces were undersized to sustain the effort of supplying troops along extended and unsecured communication lines, and the troops did not have an adequate number of supplies to fulfil their military objectives.

CONCLUSIONS

From the perspective presented, we believe that the poor application of Russian doctrine in providing logistical support contributed to the operational failure of Russian assault forces in the battle for Kyiv. The operation was planned so that the attacking forces could benefit from the element of surprise to gain ground and exploit the initiative. Initially, the execution of the plan proceeded as expected; however, it later proved that some aspects were not sufficiently planned. Thus, the rapid advance of Russian armed forces into Ukrainian territory led to an unacceptable extension of supply lines. Additionally, to achieve surprise, the attack plan was kept secret, and logistics planners did not have adequate information for supply allocation according to Russian logistics support doctrine. Furthermore,

the rapid pace of the operation resulted in deficiencies in communication systems, with messages transmitted via unsecured lines intercepted by Ukrainian armed forces, who then attacked Russian resupply convoys.

In concluding this study, we believe that the following theoretical aspects were not effectively applied to the logistical support of assault troops:

❖ According to Russian doctrine, material-technical support structures (MTO) have the primary task of maintaining combat readiness and the combat capability of troops through the efficient use of military command and control bodies, as well as MTO forces and means. In practice, Russian operational plans were kept secret from most planning staff, including logisticians. For this reason, logistical estimates were based on insufficient planning hypotheses, and combat forces carried limited amounts of supplies. The logistics effort was further strained by the needs for artillery ammunition supply, as fire support for the operation was not realized through aviation, except to a minor extent.

❖ According to the theory of the loss-of-strength gradient, as the distance of troop deployment from the base garrison increases, the combat capability of that force will decrease. Long distances of deployment imply extended supply lines that require additional protection. In the case of Russian troops, combat capability was diminished due to the lack of prior preparation of logistic structures for the resupply of ammunition and fuel. Moreover, Russian supply convoys fell into ambushes organized by Ukrainian forces, as supply line security was not established.

❖ The military transport system of the Russian Federation heavily relies on the railway network; however, for resupply, logistics focused only on road networks within Ukrainian territory. The routes used to supply approximately 15,000-20,000 soldiers were insufficient and undersized. In practice, logistical support forces failed to supply troops adequately, primarily due to the extending communication lines and a lack of access to railway infrastructure that is vital for ensuring material supplies.

We can observe that avoiding errors in the application of doctrine could have led to a different outcome in the battle for Kyiv. The lesson we consider important to be retained is the timely identification of support requirements and realistic logistical estimates, particularly through adherence to relevant doctrines and theories in the logistics field.

BIBLIOGRAPHY:

1. Berkowitz, B., Galocha, A. (2022). *Why the Russian military is bogged down by logistics in Ukraine*. *The Washington Post*, https://www.washingtonpost.com/world/2022/03/30/russia-military-logistics-supply-chain/, retrieved on 22 May 2024.

2. Boulding, K.E. (1988). *Conflict and defense: A general theory*. University Press of America.
3. Cunningham, A. (2023). *The Complexity of the Supply and Logistics System of the U.S. Army and the Need for Automation*.
4. *Doctrina logisticii întrunite a Armatei României/Romanian Armed Forces Joint Logistics Doctrine* (2023).
5. *F.T.-1, Doctrina operațiilor forțelor terestre/Doctrine for Ground Forces Operations* (2017).
6. Grau, L.W., Bartles, C.K. (2016). *The Russian Way of War: Force Structure, Tactics, and Modernization of the Russian Ground Forces*. Foreign Military Studies Office.
7. Helper, S., Soltas, E. (2021). *Why the Pandemic Has Disrupted Supply Chains*. The White House, https://www.whitehouse.gov/cea/written-materials/2021/06/17/why-the-pandemic-has-disrupted-supply-chains/, retrieved on 22 June 2024.
8. Hugos, M., Salo, E., Kuhns, R., Hazen, B. (9 August 2022). Logistics Determine Your Destiny: What Russia's Invasion is (Re)Teaching us about Contested Logistics. *Modern War Institute*, https://mwi.westpoint.edu/logistics-determine-your-destiny-what-russias-invasion-is-reteaching-us-about-contested-logistics/, retrieved on 31 August 2024.
9. *Joint Operations, Joint Publication 3-0*. (2017).
10. Jones, S.G. (2022). *Russia's ill-Fated Invasion of Ukraine*, https://apo.org.au/node/318095, retrieved on 22 June 2024.
11. Martin, B., Barnett, D.S., McCarthy, D. (2023). *Russian Logistics and Sustainment Failures in the Ukraine Conflict: Status as of January 1, 2023*. RAND Corporation, https://doi.org/10.7249/RRA2033-1, retrieved on 12 May 2024.
12. Milevski, L. (2022). *Russian Logistics and Forward Urban Defense in the Baltic States*.
13. Nistorescu, C.V. (2022). *Bătălia Kievului – considerații privind desfășurarea operațiilor militare la nivel tactic*. In *Gândirea militară românească*, 4/2022, pp.130-155, https://doi.org/10.55535/GMR.2022.4.07, retrieved on 22 August 2024.
14. Skoglund, P., Listou, T., Ekström, T. (2022). *Russian Logistics in the Ukrainian War: Can Operational Failures be Attributed to logistics? Scandinavian Journal of Military Studies*, 5(1), pp. 99-110, https://doi.org/10.31374/sjms.158, retrieved on 22 June 2024.
15. Spencer, J., Collins, L. (1 July 2022). *Waterworld: How Ukraine Flooded Three Rivers to Help Save Kyiv*. *Modern War Institute*, https://mwi.westpoint.edu/waterworld-how-ukraine-flooded-three-rivers-to-help-save-kyiv/, retrieved on 22 August 2024.
16. Ti, R., Kinsey, C. (2023). *Lessons from the Russo-Ukrainian conflict: The primacy of logistics over strategy*. *Defence Studies*, 23(3), pp. 381-398, https://doi.org/10.1080/14702436.2023.2238613, retrieved on 21 August 2024.
17. Vershinin, A. (2022). *Lessons From the Battle for Kyiv*. Russia Matters, https://www.russiamatters.org/analysis/lessons-battle-kyiv, retrieved on 22 June 2024.
18. Watling, J., Reynolds, N. (2022). *Operation Z: The Death Throes of an Imperial Delusion*.

OPERATION KURSK – ADVANTAGES, RISKS, AND DEVELOPMENT PROSPECTS FOR THE UKRAINIAN ARMED FORCES –

Lieutenant Colonel Senior Instructor Claudiu Valer NISTORESCU, PhD
Command and Staff Faculty, "Carol I" National Defence University Bucharest, Romania
DOI: 10.55535/RMT.2024.4.05

The war in Ukraine represents a significant geopolitical event, one that has the potential to reshape the European security landscape and generate a series of long-term global consequences. While the conflict is characterized by a range of troubling atrocities and destruction, it also offers insights into the creativity and adaptability of military strategies employed by the involved parties. Despite the increased transparency of the contemporary battlefield, armed combat remains an essentially human phenomenon. This is evidenced by Operation Kursk, conducted by the Ukrainian armed forces on the territory of the Russian Federation, which demonstrates that surprise, deception, operational security, and manoeuvre remain the cornerstones of land operations. These principles are creatively exploited by military commanders to gain tactical, operational, or strategic advantage.

In this context, the main objective of this study is to identify some initial lessons based on an empirical assessment of the conduct of operations. The data collection was carried out through a rigorous documentary analysis, which involved the examination of open-source information, including statements by Russian and Ukrainian officials, as well as Western analysis and studies. Furthermore, it is important to note that, in the context of an ongoing conflict, some pieces of information may be altered, incomplete, or unavailable for reasons related to information security or to the combatants' intentions to misinform and mislead, which could potentially impact the study's findings.

Keywords: operational advantages and risks; surprise; operational security; concentration of effort; Kursk;

INTRODUCTION

Following the withdrawal of Russian forces from the Kyiv area in the context of the unsuccessful large-scale offensive operation in the Belarus-North Kyiv direction and the relative stabilization of the front in the eastern and southern parts of Ukraine, there was a prevailing scepticism regarding a significant shift in the conduct of ground operations. The war of attrition appeared to favour the Russian forces that enjoyed a substantial quantitative advantage, particularly in terms of artillery systems and munitions (Martin, 2023). The Russian leadership demonstrated a notable capacity to tolerate significant casualties among own forces and disproportionate collateral damage, which proved to be a distinct advantage over the Ukrainians. However, in the early fall of 2022, the Ukrainian Armed Forces (UAF) managed to gain the upper hand by launching a complex offensive operation in the Kharkiv area of operations in the northeast of the country. The success of the counteroffensive in Kharkiv was the result of a comprehensive strategy to mislead Russian military decision-makers. This strategy involved the transfer of significant forces from the Kharkiv area of operations to the Kherson area of operations, where a potential attempt to break the front was anticipated. (Kofman, Evans, 2022). The integration of the misleading operations into the offensive operations contributed to the creation of an operational advantage that facilitated the liberation of north-eastern Ukraine (Toroi, 2023), which constituted the initial setback that would have a profound impact on the Russian Federation's *special military operation*, undermining its very foundations.

In October 2022, the city of Kherson, the only occupied regional capital, was liberated as Russian forces hurriedly evacuated the right bank of the Dnieper. The initiative had passed to the Ukrainians. However, *the partial mobilization* launched by the Kremlin regime partially solved the problems of force generation, while also setting the stage for the Russian offensive in early 2023. This new attempt to break through Ukrainian defence lines brought minor territorial gains for the Russian Federation, with the most notable success being the conquest of Bakhmut by the forces of the private military company Wagner. Despite the best efforts of the Russian commanders, who were operating under considerable political pressure, the offensive was scheduled to reach its culmination in the early spring. The initiative was to pass once again to the Ukrainian forces, who launched

the long-awaited counteroffensive in early June 2023. Its principal objective was to materialize in the south-east of the country, with the aim of cutting the land corridor linking the Crimean Peninsula to Russia. The counteroffensive did not yield the anticipated outcomes, as the battles illustrated a defining characteristic of armed conflict – *the willingness of both combatants to resort to violent means to deny their opponent's objective*. The lack of surprise resulted in predictability, while inadequate manoeuvre forces and ineffective joint planning and integration of operations also contributed to the failure of the Ukrainian counteroffensive (Watling, Danylyuk, Reynolds, 2024). Ultimately, President Zelensky was constrained to acknowledge defeat, as the reality of war is a phenomenon that combatants encounter in diverse forms and at varying levels throughout the course of warfare (Ryan, 2024). The culmination of the Ukrainian counteroffensive occurred concurrently with the loss of the initiative and its transfer to the armed forces of the Russian Federation. Subsequent to a combat algorithm cantered on artillery firepower, the Russian forces were able to gain control of several localities in eastern Ukraine, the most significant of which was Advika, a small town situated to the north of the provincial capital of Donetsk district. In May 2024, the armed forces of the Russian Federation initiated an offensive operation that caught Ukrainian defences off-guard, launching an advance from Belgorod in the direction of Vovchansk-Kharkiv. However, the Russian offensive was soon impeded by the repetition of missteps in the approach to combined arms and joint operations, as observed during the initial phase of the war. Therefore, the objective of the operation, namely the capture of Kharkiv and the establishment of a buffer zone along the border, was partially accomplished. During the summer of 2024, the persistent efforts of the Russian Federation's armed forces began to yield results along the entire front line, despite the casualties incurred. The advantage in numbers, when coupled with the tactical and technological adaptation to the new demands of the battlefield, compensated for the lack of creativity of the military commanders (Ryan, 2024). Simultaneously, the Ukrainian military has been unable to generate sufficient armed forces for almost two years of conflict, and several malfunctions or delays in the delivery of armaments and ammunition by Western states have further eroded Ukraine's defence capabilities. However, the Ukrainian armed forces have once again demonstrated their ability to surprise their enemy with a planned and executed operation that is both tactically and operationally exemplary. This operation – *Operation Kursk*, may also lead to a change in the strategic coordinates of the conflict. The Ukrainian Armed Forces (UAF) have successfully employed an operational-strategic asymmetry in this operation, effectively

transposing the physical dimension of the armed struggle to the territory of the Russian Federation and exerting unprecedented pressure on the political factor since the outset of the war. Concurrently, the Ukrainian units' actions, conducted in a manoeuvre approach, reinforce the continued relevance and significance of the offensive manoeuvre.

In this context, which is marked by large-scale combat operations on the territory of the Russian Federation, it is interesting to identify the potential lessons of this episode of the conflict. To this end, the analysis aims to empirically answer the following research questions in order to fulfil the set objectives:

- *What are the principal stages in the implementation of the offensive operation in Kursk?*
- *What are Ukraine's potential gains from territorial conquests in the Russian province of Kursk?*
- *What risks does such an operation entail for the UAF, and what are the prospects for its development?*
- *What insights can be gained from a contemporary perspective on military art?*

In order to provide answers to the aforementioned research questions, a systematic review of open-source resources was conducted, making use of existing information. In particular, we considered studies and analyses produced by Western institutes and research centres, as well as data and information presented in the media, including official statements from combatant parties or images and video recordings of combat. The potential for operational development and the identification of advantages and risks for the UAF, as well as the implications for the Russian Federation and its armed forces, were substantiated through the translation of the operational situation into a theoretical framework expressed through the benchmarks of military art. It should be noted that at the time of writing, the combat operations were still in progress. The analysis presented here covers the period from 6 August to 20 September 2024. Consequently, forecasting the potential directions in which the operation and its outcome could evolve was a challenging undertaking. It is important to note that the materialization of a given scenario is uncertain due to the inherent unpredictability and uncertainties associated with armed conflict. Additionally, operational security concerns have limited the access to information that could provide a comprehensive understanding of the entire situation. Despite these limitations, the analysis offers insights that can inform the decisions of political and military leaders, as well as the general public, about the effectiveness of the operational process at all levels.

MILESTONES REGARDING THE CONDUCT OF KURSK'S OFFENSIVE OPERATION

On 6 August 2024, Russian media sources reported that Ukrainian forces, the size and composition of which were not specified, were carrying out a large-scale incursion into the territory of the Russian Federation in the Kursk province (Evans, Mappes, Gasparyan, Wolkov, Kagan, 2024). It would seem that the Kremlin regime was not unduly concerned, given that Ukrainian forces had previously engaged in similar actions, notably in Belgorod and Bryansk provinces. Initial information from open intelligence sources indicated that Ukrainian forces were advancing in two distinct offensive directions:

- Along the state border, in the vicinity of the town of Sudzha (northeast of the Ukrainian city of Sumy);
- Along the Novenke, in the vicinity of Nikolayevo Darino.

Despite the efforts of Russian officials to downplay the significance of the incursions by the UAF, both to prevent undue panic among the population and for reasons related to the inability to fully assess the gravity of the situation, new information emerging in various Russian media outlets has indicated a continuation and intensification of the Ukrainian offensive. It follows the launch of the operation, which President Putin has described as a terrorist action (Whitmore, 2024), Ukrainian military forces have successfully secured an area of approximately 1,000 square kilometres, including the town of Sudzha and several dozen other settlements.

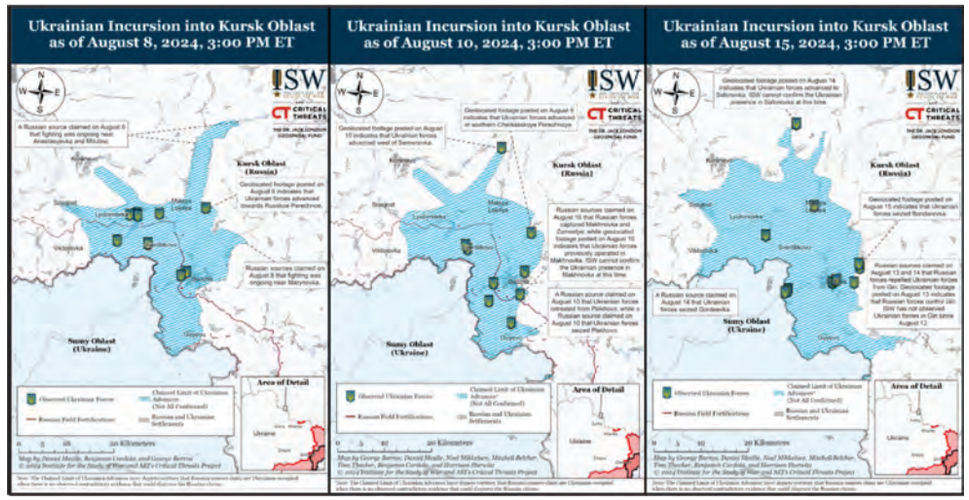


Figure 1: The operation's initial phase and the UAF advancement between 6-15 August 2024 (https://www.understandingwar.org/)

Concurrently, at the outset of the operation, Ukrainian officials were hesitant to provide insights into its objectives. It was in contrast to the efforts of the UAF, which had been assiduously striving to attain operational security – an indispensable precursor to achieving surprise and initial success. The deployment of new forces and the expansion of the conquered territory shortly after the operation's commencement indicated that the operation's nature was not characteristic of a raid-type action. In accordance with preliminary estimates, the Ukrainian military forces engaged in the offensive operation in Kursk province deployed a considerable number of troops, estimated to be in the range of several thousand, likely organized into battalion-level battle groups. Following the capture of the immediate objectives in close proximity to the state border, additional Ukrainian forces were introduced into combat, reaching a total of approximately fifteen thousand troops, comprising six manoeuvre brigades and independent battalion-level units (Axe, 2024). The operations of these units were consistently reinforced by a multitude of supporting forces, including artillery, anti-aircraft missile units, drones, electronic warfare units, and special operations forces. Concurrently, given that these units were drawn from the frontlines in the Donbas region – specifically Pokrovsk, Toretsk, and Chasiv Yar – there is substantial evidence to suggest that a large-scale operation was a highly probable course of action.

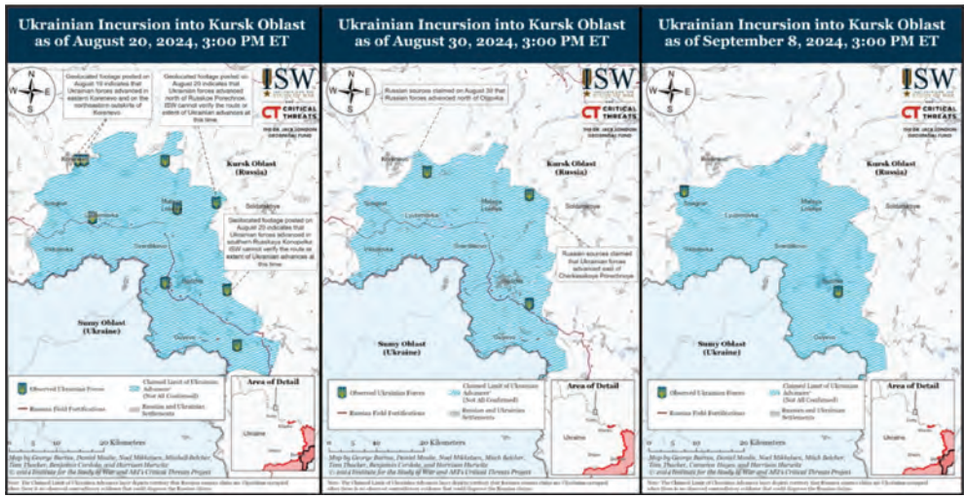


Figure 2: UAF's exploitation and objectives' consolidation 20 August and 8 September 2024 (Ib.)

In order to gain insight into the rationale behind the planning of this operation, it is necessary to conduct an analysis of the so-called *"hot spots"* on the Russian-Ukrainian front. This analysis allows two hypotheses to be put forward as to the main goals of the operation:

- weakening the offensive capacity of Russian forces in the Donbas region, specifically in the Pokrovsk offensive direction, which will be achieved by redirecting forces from the Pokrovsk offensive direction to Kursk, where they will impede the Ukrainian offensive;
- the Russian forces, engaged in an offensive operation launched in May 2024 in the Belgorod-Kharkov direction, are facing a significant threat to their right flank.

Furthermore, in one of the few interviews he gave, the commander of the Ukrainian forces, General Oleksandr Syrskyi, stated that the Russian forces were planning to launch a new offensive operation (after the one in the Kharkiv area of operations) from Kursk province in the direction of Sumi. He further states that the Ukrainian offensive operation not only diminished the Russians' capacity for further offensive action in other sectors of the front, but also prevented the implementation of a new, large-scale strike (CNN, 2024).

The relatively straightforward penetration of the UAF into Russian territory was followed by a comparable advance throughout September, as evidenced by the testimonies of Ukrainian soldiers who participated in the operation (Waterhouse, 2024). The capture of several objectives of tactical, operational, or even strategic value was achieved. They included the town of Sudzha, which serves as an important logistical hub in the area, the Gazprom-owned gas distribution station located in the vicinity of Sudzha, and tactical positions along the hard points in the terrain, which were established with the objective of consolidating territorial gains. Furthermore, in order to mitigate the efficacy of Russian forces' efforts to mount a counterattack, the Ukrainian Air Force destroyed bridges over the Seym River, thereby facilitating the consolidation of the positions they had secured to the southwest of it (Axe, 2024).

It will be of interest to observe the extent to which the objectives of the offensive operation of the UAF have been achieved, and it is to be expected that they will undergo certain transformations as events unfold. What is certain is that, in early September, the pace of the Ukrainian forces' advance slowed down. It is difficult to determine at this point whether the offensive operation has reached

its culmination, or whether this phenomenon is the result of insufficient forces and/or logistics, or the concentration of superior enemy combat power. However, Ukrainian success in Kursk is not without limits, according to RUSI military specialist Jack Watling (Watling, 2024). In the second decade of September, the Russian Federation amassed sufficient forces and undertook several offensive actions aimed at pushing Ukrainian forces back from the national territory. These actions were apparently part of a larger strategy (Strategies, 2024), which involved transferring forces from other operational areas.

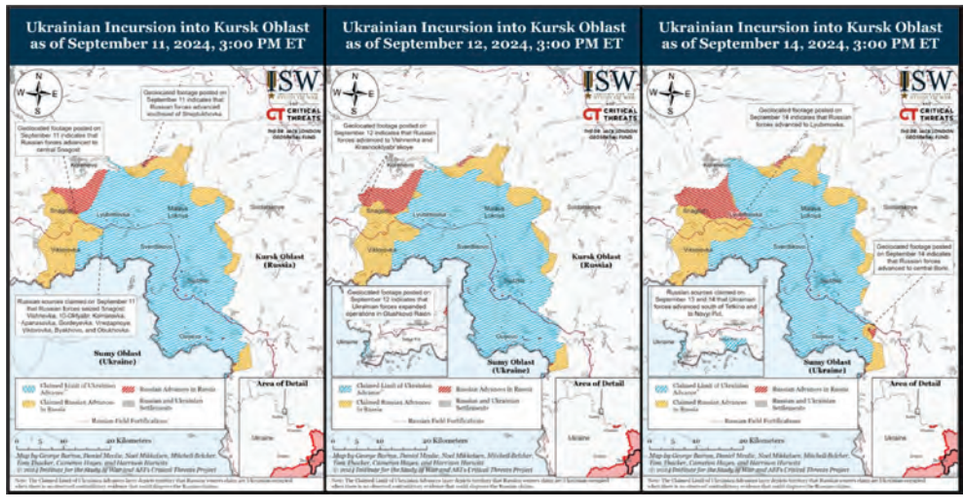


Figure 3: Counter-offensive of the Russian forces 11-14 September 2024 (Ib.)

Despite the unwavering commitment of the Russian forces, the strategies employed have resulted in only modest achievements. The active defence of the UAF, capitalizing on the advantage of favourable positions on the ground, coupled with constant harassment and rapid attacks, has fractured and thwarted the plans of the Russian commanders. It is likely that, despite the concentration of a significant number of Russian forces – approximately 40 thousand servicemen –, the decisive defeat of the Ukrainian forces in the Kursk province will be a challenging objective for the Russian Federation to achieve by the end of October, as the Kremlin regime has set itself.

ADVANTAGES AND RISKS FOR UAF AND PROSPECTS FOR THE OPERATION'S DEVELOPMENT

It is evident that Ukraine's offensive operation in the Russian province of Kursk presents a number of advantages for Ukraine, yet it also entails a number of risks. In general, military operations, and in particular combat operations, regardless of their nature and level of manifestation, generate risks. It is the responsibility of the decision-maker to identify and mitigate these risks in order to achieve the proposed objectives and create advantages. The advantages gained by the UAF as a result of the offensive operation on the territory of the Russian Federation in the Kursk province are evident at both tactical and operational levels of military operations, as well as at the strategic level, with an impact on the political dimension of the war. The same can be said of the risks.

From a tactical perspective, the Ukrainian forces were able to gain an advantage over the Russian forces. The security of operations and redeployment of several units along the frontline were effectively achieved. The offensive operation demonstrated the Ukrainian forces' capacity to integrate joint and joint manoeuvre operations, leveraging new technologies that can generate multi-domain effects. The achievement of a homogeneous and optimal mix of armoured forces and light infantry elements, supported by artillery and air defence elements, UAS (unmanned aerial system) and EW (electronic warfare) teams represented another achievement of the UAF. It resulted in the creation of the preconditions for rapid tactical successes. The ability to conquer and hold strong points on the ground represents a significant tactical advantage for the Ukrainian forces. It allows them to maintain control over the territory they have captured or to surrender it under controlled conditions, resulting in significant losses for the enemy. The flexibility of manoeuvre units to redeploy rapidly in response to changing circumstances provides the Ukrainians with a distinct advantage, as it eliminates the need to hold objectives or areas of operations with the same degree of firmness as would be required in the context of defending national territory. The persistent offensive actions undertaken with the objective of occupying advantageous tactical positions, though often only temporarily, impede the Russian forces from developing a coherent system of retaliation. The operation has not been without risks, which persist at the time of writing, particularly given the Russians' actions, which indicate their intention to move to a counteroffensive.

From a tactical perspective, the greatest risk faced by the UAF is the possibility of communication lines being disrupted, which could result in deployed units remaining encircled. Furthermore, the risk of failing to conquer and consolidate strong field alignments, thereby concluding the offensive operation, must be considered from a tactical perspective. In addition, the malfunctioning of force rotations and the inefficiency of logistical support could have a profoundly negative impact on the morale and fighting spirit of the Ukrainian military. In light of the potential for a future withdrawal of Ukrainian forces, it is crucial to underscore the necessity for meticulous coordination and planning to ensure a smooth and secure transition. It entails not only the careful orchestration of the withdrawal process through the combat apparatus but also the allocation of additional forces to guarantee its success. Such a withdrawal, however, entails a significant concentration of forces, which inevitably increases the risk of exposure to enemy air and artillery fire.

From an operational standpoint, the Ukrainian offensive actions in Kursk appear to directly support the fulfilment of Ukraine's strategic objectives. These objectives include raising the morale of the population and its own armed forces, convincing Western partners that Ukraine has not lost its determination and ability to fight, and gaining an advantageous position in future negotiations with the Russian Federation. In the near term, however, the operation has yielded tangible benefits for the Ukrainian forces, relieving pressure on those defending the Donbas region. It was not without risks, as Ukrainian commanders were tasked with the challenge of balancing the remaining defensive capabilities with those on the offensive. In this regard, the remarks of the English General Rupert Smith are edifying. In his book *The Utility of Force*, Smith emphasized that the essence of all tactics and manoeuvres, and in general the greatest tactical dilemma, is striking a balance between how much effort to expend in striking the enemy to achieve offensive objectives and how much effort to concentrate on countering his retaliation (Smith, 2019, p. 14). At the time of this analysis, the operational indicators demonstrate that the Ukrainian forces have achieved a state of equilibrium in their military operations, maintaining a balance between defensive actions in the Donbas and Kharkiv regions and offensive actions in Kursk. The achievement of the objectives set out in the offensive operation in Kursk provides the necessary conditions for the fulfilment of the existing objectives of the operations in other areas of the front. These objectives are to reduce the speed of the Russian forces' advance and to stop them in their tracks. It has been achieved by creating an operational dilemma

for the Russian political and military decision-makers, who are now required to prioritise their efforts, given that they lack the resources to sustain the pace of offensive operations and to counter a new threat. However, the dilemma created at the level of the Russian forces entailed certain costs, which in turn created risks for the UAF. The extension of communication lines necessitated the redeployment of additional Ukrainian forces to maintain and secure them. The integration of operations over time is not advantageous for the Ukrainian forces. As the deployment in Kursk persists, the combat power of the Ukrainian forces is diminished due to exhaustion and the loss of personnel and combat systems. While the ultimate outcome of the Ukrainian efforts in Kursk remains uncertain, senior officials, including President Zelensky, have asserted that the Russian counteroffensive was foreseen in the UAF's operational plan. (Galouchka, Johnson, 2024). In this regard, it seems probable that a number of criteria for measuring success, identifying the desired end-state, and realizing the transition have been established by the architects of this operation. Regardless of how the operations evolve, it can be expected that the centre of gravity of the Ukrainian forces will continue to be the manoeuvre brigades, with similar Russian structures being the only capabilities capable of defeating them.

It is important to note that the Ukrainian offensive in Kursk has a number of strategic effects at military and political levels. The tactical surprise achieved by the Ukrainians demonstrates the Russian commanders' susceptibility to deceptive operations and the shortcomings of Russian intelligence. It is counterbalanced by the strategic surprise of the Russian Federation, which saw its senior decision-makers, including President Putin, initially unable to respond, raising questions about the Russian authorities' capacity to manage such a situation (Bauer, 2024). The relocation of combat operations to Russian territory has and will continue to exert pressure on the political aspect of the Kremlin's decision-making process. The uninterrupted continuation of military operations in Donbas beyond 6 August has served to further compound the already challenging position of the Putin regime, as evidenced by statements made by the governor of Kursk province which have revealed the existence of significant divisions within the Kremlin's political system. The evacuation of local populations from occupied territories, the humanitarian crises inherent to such events, and the ineffective handling of the situation by the Russian authorities have collectively contributed to a decline in public confidence in the government. Furthermore, a considerable number of Russian soldiers have been captured, which serves as an indicator of the quality of the Russian armed

forces. Concurrently, Ukraine has established the conditions for enhancing the morale of its forces and population, while demonstrating to Western partners that it remains motivated and willing to fight.

Nevertheless, there are inherent risks associated with the potential for a tactical-operational failure of the operation, which could ultimately result in the catastrophic defeat of the UAF in Kursk and even in the capture of a significant number of servicemen by Russian forces. Such an outcome would significantly challenge the capacity of the Ukrainian military-political leadership to secure a victory for Ukraine, as the forces deployed in Kursk could prove instrumental in the defence operations in the Donbas. In this context, the severely damaged morale of the Ukrainian armed forces and population could potentially result in a collapse in several sectors of the front.

In consideration of the prospective evolution of the operation, four potential courses of action have been identified:

1. holding the conquered territory for as long as possible in order to polarize an increasing number of Russian forces, thus reducing the pressure on other sectors of the front;

2. the controlled withdrawal of the UAF from Kursk province, admitting that the objectives of the offensive operation had been achieved;

3. the defeat of the UAF and their uncontrolled and high-loss withdrawal;

4. the introduction of new combat forces by the UAF and expansion of conquered territory.

The analysis of the four courses of action reveals the interconnectivity and interdependence of the first two. The conduct of the September combat operations offers partial validation of the mentioned aspects, as evidenced by the Ukrainian decision to abandon controlled ground, thereby allowing the defending forces on the national territory to gain time. With regard to the third scenario, although the probability of its occurrence is not insignificant, it is anticipated that the Ukrainian leaders will refrain from reaching a critical juncture where the forces stationed in Kursk are no longer capable of effectively conducting defensive operations and ensuring the conditions for their withdrawal. The latter scenario is unlikely, given the acute force generation problems in the Ukrainian military and the increased likelihood of nuclear conflict escalation, with the Kursk atomic-nuclear power plant situated a distance of only 60 kilometres from the border.

CONCLUSIONS

As Winston Churchill once observed, one of the earliest insights to be derived from the ongoing Russian-Ukrainian conflict is that it would not have escalated to the point of armed conflict if each party involved had not perceived an opportunity to achieve a favourable outcome. It seems reasonable to suggest that the largest incursion of a military force into the territory of the Russian Federation since the Second World War, and its implications, will be a topic of interest for the international academic community in the future. Consequently, this event, which has the potential to be a real game-changer in the Russian-Ukrainian conflict, merits the attention of defence and security specialists. Moreover, it is a source of lessons for political and military decision-makers.

As a result of their strategic initiative, the Ukrainians have succeeded in creating a strategic asymmetry, with the military operations in Kursk province marking a first in terms of large-scale fighting on the territory of the Russian Federation. The Kremlin regime's inadequate response has resulted in tangible political and strategic challenges, undermining the reputation of the Russian Federation both within and beyond its borders. From an operational perspective, it is evident that the Russian Federation's politico-military decision-making system is still struggling to overcome a number of persistent challenges. They include an inability to effectively counter enemy misleading operations, a lack of prompt and coherent response from local and governmental authorities to unexpected threats, a tendency to overlook humanitarian concerns, and a delayed reaction by military commands in adjusting operation plans and adapting to new circumstances. Furthermore, in the near future, the Kremlin regime will be required to redirect its efforts in order to effectively address similar threats in other border areas. It will inevitably result in a significant strain on special military operation forces, and it is plausible that a new mobilization of the population may be necessary.

Concurrently, the Ukrainian forces were able to enhance the morale of the troops and the local population, which had been significantly impacted by a lack of sufficient forces and ammunition, limited opportunities to replace units at the front, persistent retreat along the main forbidden routes, and frequent exposure of the population to enemy rocket and artillery fire. From an operational standpoint, over a month after the initiation of the operation, the desired effects appear to be manifesting. The pace of the Russian offensive in the Donbas area of operations, including in the direction of Pokrovsk, has notably decelerated

due to the redeployment of forces to impede the advancement of Ukrainian forces in Kursk. The initial success of the operation demonstrates not only the ability of the Ukrainian commanders to plan and execute large-scale offensive operations in a creative manner, but also the determination and motivation of the Ukrainian soldiers. As a result, the operation has made a significant contribution to securing the support of Ukraine's Western partners.

The hostilities that occur, regardless of their scale, validate the essential milestones of the operational process, which represents the essence of armed combat. Armed combat is, by definition, a human phenomenon. As a result, the primary objective of any combatant is to gain an advantage over their opponent. It is achieved through the use of tactics designed to mislead and catch the enemy off-guard. These principles, which have been demonstrated to be effective in the context of the FAU operation, serve to enhance offensive operations and create conditions that favour success.

Another principle that has been shown to be relevant in this context is operational security. This is an essential prerequisite for the concentration of forces and assets in the context of increased battlefield transparency. The strategic manoeuvre and the tactical approach to the operations, amplified by the mission command, facilitated the Ukrainian forces a relatively easy penetration of the Russian forces, the development of the operation, the exploitation of the success, and the generation of the collapse of the defence lines. These foundational elements of ground operations continue to serve as a defining condition of the operational process. The achievement of sufficient combat power was contingent upon striking an optimal balance of manoeuvre-fire-protection functions, all of which were enhanced by a flexible and efficient command and control system of the Ukrainian forces. Furthermore, anticipation of the enemy's actions and exploitation of its vulnerabilities, both systemic and mental, enabled the Ukrainians to rapidly develop offensive operations. In a matter of weeks, they conquered an area equivalent to the Russian gains made throughout 2024.

At this stage, it is challenging to anticipate the ultimate result of Operation Kursk. However, Western military forces can undoubtedly capitalize on the benefits of shifting the locus of military operations to enemy territory, even if this is only a temporary or spatially limited manoeuvre. Therefore, with regard to the development and calibration of tactical force structures, it is our belief that the development of doctrines and concepts of operation should be aimed at achieving

an optimal balance between defensive and offensive capabilities. It will ensure a comprehensive and versatile military response capability, which will provide the armed forces with superiority in space and time and in all fields of operation.

BIBLIOGRAPHY:

1. Axe, D., *"Ukraine Is Blowing Up Bridges in Kursk as Fast as Russia Can Build Them",* Forbes, retrieved on 21 August 2024.
2. 2. Biddle, S. *"Ukraine and the Future of Offensive Maneuver"*, 18 November 2022. War on the Rocks
3. Bradley, M., https://www.rand.org/multimedia.html; https://www.rand.org/. 23.05.2023; https://www.rand.org/multimedia/video/2023/05/23/ukraine-is-running-out-of-ammo-the-West-doesnt-have-enough.html, retrieved on 9 August 2024.
4. CNN, https://edition.cnn.com/2024/09/08/; https://edition.cnn.com/, 14.09. 2024; https://edition.cnn.com/2024/09/08/europe/amanpour-general-oleksandr-syrskyi-interview-read-transcript-intl/index.html, retrieved on 20 September 2024.
5. Evans, A., Mappes, G., Gasparyan, D., Wolkov, N., Kagan, F.W., https://understandingwar.org/research, 06.08.2024; https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-august-6-2024, retrieved on 20 September 2024.
6. Galouchka, A., Johnson, L. *"Russian counteroffensive in Ukrainian-controlled Kursk begins says Zelensky".* Washington Post 21 July 2024.
7. Kofman, M., Evans, R. *"Ukraine's Kharkiv Operation and the Russian Military's Black Week".* War on the Rocks.
8. Lee, R., Kofman, M. *"Not Built for Purpose: The Russian Military's Ill-Fated Force Design".* War on the Rocks, 22 June 2022.
9. Ryan, M. *"Russia's Adaptation Advantage".* Foreign Affairs. – *"The misfortunes of war"*. The Engelsberg Ideas, 2 July 2024.
10. Smith, R. (2019). *The Utility of Force*. London: Penguin Random House.
11. Strategies, Centre for Defence, https://cdsdailybrief, 16 September 2024, https://cdsdailybrief.substack.com/p/russias-war-on-ukraine-160924, retrieved on 21 September 2024.
12. Toroi, G-I., Stanciu, C.-O (2023). *Aspecte privind planificarea acțiunilor de inducere în eroare la nivel operativ*. In *Gândirea militară românească*. București: Statul Major al Apărării, no. 3, pp. 20-45.
13. *Two More Ukrainian Air Assault Brigades Have Joined the Invasion of Russia*, Forbes, 14 August 2024.
14. Waterhouse, J., https://www.bbc.com/news, 13 August 2024; https://www.bbc.com/news/articles/cze5pkg5jwlo, retrieved on 21 September 2024.
15. Watling, J. *"Ukraine's extraordinary incursion into Kursk has changed the narrative of the war – but is a high-risk strategy".* The Guardian, 17 August 2024.

16. Watling, J., Danylyuk, O.V., Reynolds, N. (2024). *Preliminary Lessons from Ukraine's Offensive Operations, 2022-23*. Research Report, Royal United Services Institute.
17. Whitmore, B., https://www.atlanticcouncil.org/blogs, 15 August 2024; https://www.atlanticcouncil.org/blogs/new-atlanticist/ukraines-kursk-offensive-marks-putins-third-major-humiliation-of-the-war/, retrieved on 20 September 2024.
18. https://www.understandingwar.org/, retrieved on 22 September 2024.

THE IMPORTANCE OF GEOINT IN SUPPORTING MILITARY ACTIONS IN UKRAINE

Lieutenant Colonel Cristian PANAIT, PhD
"Henri Coandă" Air Force Academy, Brașov
DOI: 10.55535/RMT.2024.4.06

Geospatial Intelligence (GEOINT) has proven to be a crucial component in modern warfare, especially in the context of the conflict in Ukraine. This paper aims, through documentation, to evaluate and analyse the applications, impact, and strategic significance of GEOINT in creating and developing an accurate image of the area of operations for supporting military actions in Ukraine.

The Russo-Ukrainian conflict serves as a case study to determine how GEOINT contributes to data fusion and the necessary information for the targeting process, as well as the monitoring, assessment, and validation of military courses of action, particularly in the decision-making process. By analysing perspectives from various sources, this article underlines the importance of GEOINT in contemporary military strategy and its implications for future conflicts.

Keywords: GEOINT; Ukraine; modern warfare; data fusion; Big Data;

INTRODUCTION

The ongoing conflict in Ukraine has brought to the forefront the evolving role of Geospatial Intelligence (GEOINT) in military operations. As an intelligence discipline, GEOINT uses data from diverse geospatial sources such as satellite imagery, drone surveillance, and Geographic Information Systems (GIS), to generate actionable intelligence. This intelligence involves analysing spatial images and data to understand military movements, landscape structures, and human activities on a broad geographical scale.

In the Ukraine conflict, GEOINT has been widely used for strategic mission planning, real-time monitoring, and evaluating military actions. By fusing commercial satellite images, drone surveillance, and open-source intelligence (OSINT), the battlefield has become more transparent, enabling the parties involved to adapt their strategies and quickly respond to changes on the ground. This adaptability and rapid reaction are essential in modern warfare, where battlefield dynamics can be extremely swift and unpredictable.

Authors such as Dr. Robert Clark (NDS Show, 2023), a long-standing expert in geospatial intelligence, or Michael J. Ard and Jack O'Connor from Johns Hopkins University (2022), have analysed the implications and progress of GEOINT in the Ukraine conflict, providing crucial perspectives on the changing nature of intelligence gathering and its strategic use in warfare. These insights highlight the need for modern armies to enhance their geospatial analysis capabilities to gain a strategic advantage in future conflicts.

The importance of GEOINT in creating a precise (both unique and local) aerial image for military actions in Ukraine and detailing how the integration of GEOINT has influenced the Ukrainian armed forces' ability to adapt to the war's dynamic nature, information fusion, and collaboration between geospatial intelligence agencies have been an essential support to Ukraine's defence efforts.

THE ROLE OF GEOINT IN UKRAINE'S MILITARY OPERATIONS

To understand the role of GEOINT in Ukraine's military operations, it is necessary to acknowledge the foundation upon which GEOINT is built: *"GEOINT is an intelligence discipline and a tradecraft that evolved from the integration of imagery, imagery intelligence (IMINT), and geospatial information"* (National Geospatial-Intelligence Agency, 2006).

From this perspective, the Ukraine conflict serves as a case study for modern warfare, where GEOINT plays a vital role in the collection, processing, and dissemination of geospatial data to support military actions. This role includes providing real-time aerial imagery, analysing enemy troop movement patterns, identifying artillery positions, and monitoring critical infrastructure. Therefore, GEOINT's capability is extremely effective in offering a comprehensive view of the battlefield and is highly efficient in enabling Ukrainian forces to make strategic decisions perfectly adapted to the realities on the ground.

Data Fusion

The use of GEOINT *"products"* in the Ukraine conflict has been conditioned by the implementation and development of capabilities to integrate information from multiple sources. Ukraine's command, control, and intelligence systems, mentioned by the United States Geospatial Intelligence Foundation (USGIF), use data from commercial satellites, drones, smartphones, and social media platforms to create an accurate aerial image. This fusion of information includes combining high-resolution satellite images with ground-collected data from both civilians and military personnel. In this way, a detailed picture of the real-time situation is created, which can be used to guide tactical and strategic decisions.

GEOINT has also enabled Ukrainian forces and their allies to monitor enemy troop movements, identify strategic targets, and optimize military operations. Satellite images, together with geospatial analyses, have provided real-time information on battlefield changes, identifying adversary positions and elements of critical infrastructure. These data have been used to precisely guide artillery and missile actions, coordinate drone flights, prevent surprise attacks, and minimize civilian casualties.

In the process of collecting and integrating data from multiple sources, commercial satellites play an essential role. Companies such as Maxar, ICEYE, and Capella have provided high-resolution images that allow the identification of Russian troop positions, military equipment, and critical infrastructure. The pieces

of data collected by these companies are then analysed in the context of other information sources, such as drone images, on-ground reports, and communication service data. This integrative approach allows Ukrainian forces to obtain a clearer perspective of the situation, offering a strategic advantage in anticipating and countering enemy movements.

The importance of information fusion becomes evident when looking at how Ukraine has managed data sharing and coordination with its allies. According to USGIF, the Ukrainian armed forces have used a communication system that enables the rapid sharing of on-ground information with both national military structures and international partners. This *"hyperconnectivity"* of information exchange facilities has led to efficient collaboration between different command levels, thus ensuring better coordination of operations.

In addition, international partnerships have played a vital role in providing geospatial data and building Ukraine's analytical capabilities. Vice Admiral Robert Sharp (National Geospatial-Intelligence Agency-1) underscores the role of the National Geospatial-Intelligence Agency (NGA) in facilitating the sharing of intelligence data, and providing training and support for using geospatial intelligence platforms. These partnerships have strengthened Ukraine's position against Russian aggression and provided a model for future collaborations in similar conflicts.

Civilians have also become a valuable source of information, contributing to data fusion in the GEOINT system. Images and videos taken with smartphones, as well as on-the-ground reports, have been analysed to validate and complement data collected by other means. This civilian participation has added an additional level of situational awareness, which is difficult for Russian forces to counter. Additionally, Open-Source Intelligence (OSINT) has provided access to a wide range of information, from military vehicle movements to artillery equipment positioning, contributing to a more informed decision-making process.

Targeting and Big Data on the Battlefield

GEOINT has become an essential tool for the targeting process in the Ukraine conflict. Data obtained from SAR satellites, such as those provided by ICEYE and Capella, and from radio-frequency systems, like HawkEye 360, have enabled Ukrainian troops to accurately locate and strike enemy targets. This capability to obtain exact information about the enemy's position and movements has been crucial for Ukraine's operational success.

Another important aspect of GEOINT's use in Ukraine is collecting and analysing *"Big Data"* from the battlefield. As Dr. Robert Clark (NDS Show, ib.) highlights, data collected from drones, satellites, smartphones, and other sources are processed using artificial intelligence to speed up the decision-making cycle. Thus, the *"Observe-Orient-Decide-Act"* (OODA) cycle is accelerated, allowing Ukrainian troops to make decisions more quickly and informed than their adversaries.

A critical role in providing on-the-ground information has been played by civilians who have used smartphones to collect and send geospatial data, thereby expanding the targeting process of the Ukrainian armed forces. This involvement of civilians not only extends the reach and precision of the targeting process, but also adds an element of operational flexibility that is difficult for enemy forces to counter. However, this approach also presents risks, as civilians may become targets if identified as information providers.

Validation and Monitoring of Military Movements

GEOINT has played a central role in validating and monitoring military movements, offering Ukraine a powerful tool for anticipating and countering enemy strategies. This continuous monitoring capability of the battlefield has provided essential information for both defence and attack operations.

One of the most valuable GEOINT contribution to this conflict has been monitoring Russian troop movements and military equipment. Jack O'Connor (John Hopkins University) points out that, through satellite imagery and radar data, Ukrainian forces could observe the troop concentrations, the deployment of heavy equipment, and the logistical movements of the enemy. This information has been used to adjust defence strategies, prepare ambushes, and coordinate attacks on the weak points of Russian forces.

After each attack, Ukrainian forces have used GEOINT to assess the damage caused and determine the effectiveness of the strikes. Satellite images provided by commercial companies such as Maxar have been analysed to identify destroyed vehicles, fortified positions, and changes in the terrain structure. The assessment has been crucial in determining whether a target was neutralized or if further attacks were necessary. Additionally, damage assessment has provided critical information for the tactical improvement of future operations.

GEOINT has also served as a validation tool for information from other sources, such as OSINT and ground reports. In an operational environment where misinformation and information warfare are widely used strategies, the ability

to independently verify reports is vital. Satellite imagery and radar data have been used to confirm or refute claims related to troop movements, enemy positions, or damage extent. This validation has improved the quality of information available to military and political decision-makers, providing a more solid basis for decision-making.

Apart from monitoring military movements, GEOINT has been used to oversee critical infrastructure, such as nuclear power plants, dams, transport networks, and fuel depots. This monitoring has been essential to detect potential threats and ensure the protection of these assets. It has also allowed Ukrainian authorities to plan emergency actions in the event of an attack on these infrastructures, thus contributing to national resilience in the face of aggression.

STRATEGIC AND FUTURE IMPLICATIONS OF GEOINT

The successful use of Geospatial Intelligence (GEOINT) in Ukraine has extensive implications, both for current military operations and for future conflicts. The Ukraine conflict has demonstrated that GEOINT is not just a support technology but also a fundamental element that can change the dynamics of warfare. This chapter details the strategic implications, including international collaborations, technological integration, and the need to redefine global military strategies.

Collaborations and Partnerships

One of the most significant lessons learned from the use of GEOINT in Ukraine is the importance of partnerships and international collaboration. In the context of the conflict, cooperation between Ukraine and its allies from NATO and other international organizations has enabled the rapid mobilization of resources and geospatial data. These collaborations have highlighted that no country can fully develop or exploit GEOINT technologies in isolation. Instead, success depends on the efficient exchange of data and expertise among nations, intelligence agencies, and the private sector.

Vice Admiral Robert Sharp (National Geospatial-Intelligence Agency-2), emphasizes that these partnerships are essential for providing real-time situational awareness to military commanders and political decision-makers. Collaborations between NGA and international partners have included sharing satellite images, radar data, and image analyses to create a complete operational picture of the battlefield. This information-sharing has facilitated faster and better-informed

responses to dynamic changes on the ground, which proved vital in the Ukraine conflict.

In addition to governmental partnerships, collaboration with the private sector has been also crucial. Companies such as Maxar, ICEYE, and HawkEye 360 have provided access to commercial satellite images and essential geospatial data for military operations. Maxar, for example, provided high-resolution images that helped identify Russian military positions and monitor their movements. These private companies have become key players in the global GEOINT ecosystem, providing advanced technologies that complement and extend the capabilities of government agencies.

Another important dimension of collaboration has been the interaction with the academic environment. Universities and research institutes have provided expertise and developed new methodologies for geospatial data analysis while preparing the next generation of GEOINT analysts. Vice Admiral Sharp praises the role of the academic community, stating that top-tier education and research are essential for enhancing GEOINT capabilities. Research partnerships have led to the development of advanced technologies, such as artificial intelligence applied to image analysis, which has enabled the rapid interpretation of large volumes of collected data.

Technological Integration and Adaptation

The integration of various geospatial technologies into a single operational structure has been essential for Ukraine's success on the battlefield. The ability to gather and analyse data from multiple sources, including satellite imagery, radio signals, radar data, and drone information, has allowed the Ukrainian armed forces to obtain a comprehensive perspective of the situation on the ground.

This integration has required the rapid adaptation of existing technologies and the development of new analytical tools. Dr. Robert Clark points out that, in the past, the intelligence cycle was divided into distinct phases – *collection, processing, analysis, and decision-making*. In the modern context of the Ukraine conflict, this cycle has become much more fluid, allowing real-time collaboration between collectors, analysts, and decision-makers. This collaborative approach has led to a more efficient process of geospatial data collection and interpretation, thus accelerating military decision-making.

A remarkable example of this integration is the use of artificial intelligence (AI) algorithms for processing and analysing satellite images. AI has been used to detect patterns in troop movements, identify targets, and assess target effects. By using

AI, Ukraine has managed to significantly reduce the time required for data analysis, providing military commanders with information in a very short time. Furthermore, AI-based predictive models have allowed for anticipating enemy movements, thus providing a strategic advantage on the battlefield.

The integration of commercial technologies, such as drones and civilian communication platforms, has also contributed to operational success. Ukraine has used drones to collect data in inaccessible or dangerous areas, while commercial communication networks have been used to quickly transmit this data to command centres. For example, the Starlink platform, provided by SpaceX, was used to ensure stable and secure communications in areas where traditional infrastructure was compromised. These commercial technologies have been integrated into a military communication system in which information could be quickly transmitted to troops on the ground.

Technological adaptation has not been limited to integrating new tools as it has also included the development of innovative tactics. For example, the use of geospatial data by civilians to provide information on enemy positions have enabled extensive effects, whereby armed forces can use crowdsourced data to identify and strike targets. This decentralized approach has significantly extended Ukrainian forces monitoring capability and added a level of adaptability difficult for Russian forces to anticipate.

Implications for Military Strategy

The Ukraine conflict has underscored the need for military forces to revise and modernize their strategies to better integrate geospatial intelligence. In the past, GEOINT was considered a niche field, used primarily for reconnaissance and mapping missions. However, the Ukraine conflict has demonstrated that GEOINT can fundamentally change the course of modern warfare, providing critical real-time advantages.

A key aspect of this strategic shift is recognizing the importance of informational superiority. Geospatial intelligence offers a level of situational awareness that cannot be reproduced by other means. The ability to monitor enemy movements in real time, assess target effects, and foresee future actions provides a strategic advantage that can determine the outcome of a conflict. However, this information superiority requires ongoing investments in GEOINT technologies and in training the personnel to efficiently exploit these resources.

Integrating GEOINT into military strategy also requires a shift in how military operations are organized and conducted. Traditionally, collecting and analysing geospatial information were centralized tasks managed by national intelligence agencies. The Ukraine conflict has shown that these processes need to be decentralized to respond quickly to changes on the battlefield. It means that every military unit, from the tactical to the strategic level, must have access to relevant geospatial data and be able to make decisions based on it.

Furthermore, the use of GEOINT in the context of the Ukraine conflict has raised questions about the future of conflicts in which non-state actors, including private companies and civilians, play a significant role in collecting and disseminating information. Armed forces must develop strategies to coordinate these resources and ensure information security in an increasingly interconnected environment. In this regard, collaboration with the private sector and the academic community has become essential to develop the technologies and tactics necessary for the complete exploitation of GEOINT.

CONCLUSIONS

By detailing how GEOINT has been used in information fusion, targeting, and monitoring the military movements, it has become clear that this discipline has played an essential role in Ukraine's defence strategy. The integrated use of geospatial technologies has allowed not only for tactical advantages on the battlefield but also for the development of adaptive strategies that have contributed to Ukraine's resilience and operational success.

The Ukraine conflict has changed the paradigm of GEOINT use, demonstrating that it is essential for achieving and maintaining informational superiority in modern warfare. By integrating data from multiple sources and collaborating with international partners, Ukraine has managed to create a detailed operational picture of the battlefield, facilitating rapid and adaptive responses to changes on the ground. The implications for global military strategy are profound, highlighting the need to invest in geospatial technologies, develop partnerships, and re-evaluate tactics and organizational structures to address the challenges of modern warfare.

BIBLIOGRAPHY:

1. AFCEA Signal (n.d.). *U.S. GEOINT Clear Driver in Ukrainian Defense*, https://www.afcea.org/signal-media/intelligence/us-geoint-clear-driver-ukrainian-defense, retrieved on 15 September 2024.

2. Barramou, F., El Brirchi, E.H., Mansouri, K., Dehbi, Y. (2022). *Geospatial Intelligence: Applications and Future Trends*. Springer.
3. C4ISRNET (25 April 2022). *How One U.S. Intelligence Agency is Supporting Ukraine*, https://www.c4isrnet.com/intel-geoint/2022/04/25/how-one-us-intelligence-agency-is-supporting-ukraine/, retrieved on 28 September 2024.
4. DGI (n.d.). *Geospatial Intelligence Partnerships during the Russia-Ukraine War*, https://dgi.wbresearch.com/blog/geospatial-intelligence-partnerships-during-russia-ukraine-war, retrieved on 28 September 2024.
5. European Security&Defence (March 2023). *Understanding the View: Imagery in Geospatial Intelligence*, https://euro-sd.com/2023/03/articles/30037/understanding-the-view-imagery-in-geospatial-intelligence/, retrieved on 4 September 2024.
6. GMFUS (n.d.). *Geospatial Technology's Role in the Conflict in Ukraine*. The German Marshall Fund of the United States, https://www.gmfus.org/news/geospatial-technologys-role-conflict-ukraine, retrieved on 8 September 2024.
7. Johns Hopkins University (14 March 2022). *The Geospatial Intelligence Perspective on Ukraine*, https://hub.jhu.edu/2022/03/14/michael-ard-john-oconnor-geospatial-intelligence/, retrieved on 28 September 2024.

THE USE OF UNMANNED SYSTEMS IN MARITIME CONFINED SPACES

Navy Captain Valentin-Marian TOMA
Commander of "Mărășești" Frigate, Constanța, Romania
DOI: 10.55535/RMT.2024.4.07

Unmanned systems, commonly referred to as drones, are widely used for surveillance, research, protection of military and civilian targets, search and rescue, and are becoming an increasingly important part of the maritime domain as they are used to execute tactical combat actions in air, surface and sub-surface combat environments. The successful use of unmanned systems in tactical combat actions in the war in Ukraine is leading to the rapid innovations in this field, which also implies the adoption of new tactics and strategies for their use in combat. In this article we have analysed the use of drones in the conflicts in the Black Sea and the Red Sea in order to highlight the importance to be given to the development of this field, especially for the limited maritime spaces, where the relatively small distances between targets represent a good opportunity to operate unmanned systems. The use of unmanned systems in maritime confined spaces covers a wide range of missions with the advantage of using them over a long period of time, at relatively low cost, and without jeopardizing human resources.

Keywords: drone; combat environment; tactical combat actions; maritime space; lines of communication;

INTRODUCTION

The success of the use of unmanned systems in the military conflict between Ukraine and the Russian Federation and in the actions of the Houthi rebels in the Red Sea against merchant ships has generated increased interest from the armed forces of countries in the vicinity of the conflict zones, but also from countries that have realized that in future conflicts, the effectiveness of strikes must be increased at the lowest possible cost and with limited exposure of human resources. The capabilities of unmanned systems are improving exponentially due to technological progress, becoming more affordable, which means that more potential adversaries have access to this technology, extending a wider range of asymmetry in tactical actions conducted in air, surface and subsurface combat environments. The research methods I will use in this paper are predictive, as this field of unmanned systems is in a constant state of flux, and the case analysis derives from the use of these air and naval unmanned systems in conflicts in the Black Sea and Red Sea.

The strategy of using unmanned systems/drones in confined maritime spaces, such as enclosed or semi-enclosed seas, differs considerably from the use of these systems in the open ocean, the determining factor being space, an element that must be considered in terms of geographical setting in relation to the maritime littoral space, size and configuration of the coastline, hydrographic and oceanographic characteristics, degree of industrialization of coastal areas and size of coastal urban areas.

SPECIFIC CHARACTERISTICS OF MARITIME CONFINED SPACES

In limited maritime spaces, it is a strategic challenge for a littoral nation to conduct its own naval operation. Manoeuvring space depends on the length of maritime boundaries, the size and characteristics of the water surface, international agreements and the size of the fleet. A country's naval power in enclosed and semi-enclosed seas is influenced by the configuration of the coastline, the number and characteristics of ports, the possibilities for exploiting natural resources, economic development and technological progress. The term enclosed or semi-enclosed sea means *"a bay, basin or sea surrounded by more than one State and connected to another sea or the ocean by a narrow passage or formed wholly*

or mainly by the territorial seas and exclusive economic zones of several States" (UNCLOS, United Nations, p. 53).

The military analysis of maritime confined spaces can be based on spatial, action, temporal and informational criteria (Nistor, Scipanov, 2021, p. 27). These criteria were established based on the distance to targets, the intensity of military actions, reduced action times, speed of action, as well as real-time realization of the Recognized Maritime Picture/RMP. The physical characteristics of the littoral zone and the open spaces between localities determine the organization of the littoral defence through the positioning of forces and assets. In this context, Professor Milan Vego of the US Naval War College, Newport, Rhode Island, states that: *"future wars at sea will predominantly be fought near the littoral"*, which leads us to the rather high probability that these wars will be fought in maritime confined spaces, such as enclosed or semi-enclosed seas (Vego, 2007, p. 14).

The maritime spaces in the coastal zone provide, to a large extent, the necessary conditions for the use of fast surface ships, aerial drones, naval drones and underwater drones, mainly using swarming tactics, attacks from several directions in order to gain control of the sea or to deny the sea in the maritime space in question.

The maritime space controlled by a naval power becomes a dynamic factor from the moment naval tactical actions at sea are initiated. It is enlarged by actions on the enemy, forcing him to restrict the area of operations, or it can be reduced if the enemy is superior in quality and quantity.

The Black Sea has access to the Planetary Ocean through the Turkish Straits (Istanbul and Çanakkale). It is thus considered a semi-enclosed sea, with an area of 423,000 km^2, with a maximum east-west length of 687 Nm (nautical miles) from the shore of the Bay of Burgas (Bulgaria) and the mouth of the Inguri River in Georgia, and a minimum width at the meridian of the southern tip of the Crimean Peninsula (Cape Sarici) of 142 Nm. (Pontic Itineraries/Naga Sea). The maximum depth of the Black Sea is 2,212 m, with an average depth of 1,197 m (Vespermeanu, 2005, p. 29), compared to the Baltic Sea, which has, on about 60% of its surface, a depth of less than 150 m, and the North Sea, with an average depth of 100 m. To give a more detailed picture of the size of the semi-enclosed seas, it should be noted that the Baltic Sea is 920 m long and 105 m wide, the North Sea is 700 m long and 420 m wide at its widest, and the Mediterranean Sea is the largest in terms of surface area – 2,500 m and with a maximum width of around 1,000 m (Ib.).

The characteristics of the seas presented above lead us to the conclusion that the employment of considerable forces in confined sea spaces most likely does not ensure that surprise will be achieved, but the use of aviation and unmanned

systems can achieve surprise and gain control of the sea for a certain period of time. Thus, the use of unmanned systems in confined maritime spaces can limit or even prohibit the enemy's use of large ships such as destroyers or frigates, thus increasing the likelihood of military action as close to the enemy shore as possible.

In enclosed and semi-enclosed seas, water depth is the main criterion in the use of submarines, since the transparency of the water at certain time of the day makes it possible to detect a submarine in the air at depths of more than 50 meters during daylight. Both aviation and unmanned aircraft/UAV (Unmanned Aerial Vehicle) can be successfully used to carry out aerial surveillance of maritime areas.

The transmission of sound through water in shallow seas is strongly influenced by the characteristics of the underwater relief and thermal gradients in the surface layers, therefore it is necessary to know the climatological factors (wind, waves, air temperature, water temperature, precipitation period, cloudiness, fog) for the efficient use of surface and underwater sensors on board a ship. From the analysis of depth, salinity, water transparency and submarine relief, it is possible to create a picture of the forces and means that can act in such a maritime space.

I believe that in confined maritime spaces, electronic warfare, limited tactical naval actions, short- and medium-range vectors, and the use of all types of unmanned systems in combat environments are predominantly employed to obtain, maintain/contest sea control. Economic objectives and military objectives of tactical or operational level are primarily targeted, so that the achievement of these objectives will lead to the fulfilment of the strategic objective.

The relatively small distances between the combatant countries bordering a limited maritime space may facilitate certain surprise tactical naval and tactical air actions by the numerically inferior side against enemy naval and land targets with a high probability of success. The actions of Ukrainian special forces against land or naval targets belonging to the Russian Federation, using unmanned air or naval systems, validate the hypothesis that technological development and rapid adaptation of combat tactics to new situations in the theatre of operations is a viable solution today, and in the near future the role of unmanned systems will constantly increase.

Of the major naval powers, the Russian Federation is in the most unfavourable position, says Geoffrey Till, in *A Guide for the Twenty-First Century*, as the Black Sea, the Baltic Sea and the Sea of Japan exits are controlled by traditional adversaries. In this regard, he quotes Russian Admiral Sergey Georgiyevich Gorshkov, former commander of the Soviet Union Navy, who emphasizes that: *"the difficulty for Russia,*

as a maritime power, lies in its geographical position, a position which calls for the existence of an independent fleet capable of operating in all four possible maritime theatres of operations". (Till, 2013, p. 114) At present, the Russian Federation has favourable access to the Planetary Ocean through the Barent Sea and the Sea of Kamchatka, areas where it has major naval bases.

In support of the claim that the Russian Federation does not have free access to the Planetary Ocean through the Black Sea comes Türkiye's decision in February 2022 to ban warships belonging to the Russian Federation and Ukraine from transiting the Turkish Straits on the basis of the provisions of the Montreux Convention, as a result of the armed conflict between the Russian Federation and Ukraine. The Montreux Convention gave Türkiye the right to militarize the straits area in a situation of armed conflict (Moraru, 2011, p. 7).

The integration of Finland and Sweden into the North Atlantic Alliance/NATO has turned the Baltic Sea into a sea surrounded, for the most part, by Alliance member countries, thus leaving the Russian Federation with only the enclave of Kaliningrad and the eastern part of the Gulf of Finland.

The Black Sea is the maritime space surrounded by the coasts of three North Atlantic Alliance member states (Romania, Bulgaria and Türkiye), one aspiring NATO member (Georgia) and the two countries in armed conflict, the Russian Federation and Ukraine. This maritime space provides an important corridor for the transportation of goods from the European Union to Asia, the transportation of cereals from Ukraine to Africa and, possibly, for ensuring energy security for the riparian states or, at least, reducing energy dependence on the Russian Federation (Ciorobea, 2024).

From the above it can be concluded that, in maritime confined spaces/enclosed or semi-enclosed seas, unmanned systems can be used to execute a wide range of missions in all environments (air, surface and sub-surface water).

The use of unmanned systems in maritime confined spaces is favoured by the following characteristics:

- relatively small distances between targets;
- possibility of enemy surprise;
- possibility of executing attacks from several directions;
- real-time recognized maritime picture;
- possibility to accurately assess the effect on the target;
- possibility of combining air, land, naval strikes with strikes executed by unmanned systems;

- particularly high operational effort to combat threats generated by unmanned systems;
- the manufacturing costs are relatively low for unmanned systems compared to the costs incurred for the manufacture of conventional military equipment and munitions (airplanes, ships, tanks, missiles, torpedoes, projectiles etc.).

SHAPING THE OPERATIONAL ENVIRONMENT IN MARITIME CONFINED SPACES USING UNMANNED SYSTEMS

In this chapter I will highlight how unmanned systems can shape the operational environment by analysing some of the military actions deployed in the maritime space of the north-western Black Sea by the Russian Federation and Ukraine.

The Russian Federation's aggression against Ukraine has turned the northern Black Sea into a maritime space where both combatant countries are trying to exert control over the sea. By the exercise of this control is meant *"the ability to use a part of the ocean/sea and related airspace for military and non-military purposes and to prohibit the enemy from using this area for a period of time"* (Vego, 2016, p. 26).

For Ukraine, it is vital to ensure freedom of navigation for its own and neutral merchant ships, so that grain exports can take place, and to disrupt the sea lines of communication of vessels belonging to the Russian Federation. By the use of the phrase *sea lines of communication* is meant *"ports and navigable routes between ports with specific navigational arrangements and transport vessels using these routes"*. (Hanganu, 1998, p. 194). The Russian Federation aims to block Ukrainian grain shipments and to occupy favourable positions at sea from which to launch missile attacks on the Ukrainian coast.

As early as 24 February 2022, the date of the invasion of Ukraine by the Russian Federation, the Russian Black Sea Naval Forces had more and far superior ships in terms of technical and armament equipment. Apparently, gaining and maintaining sea control in the northern Black Sea area was not a problem, as the Ukrainian Navy focused on planting mine barrages in the littoral zone and deliberately sank the largest warship in its inventory in order to prevent it from being taken over by the Russians. In the first part of the armed conflict, the Russian Navy gained sea control in the northern Black Sea area and the Russian Naval Forces even occupied the Snake Island (an island that belonged to Ukraine) on 24 February 2022, and started to notify on VHF Channel 16 (international emergency channel) all merchant ships that the Russian Federation was conducting a counter-terrorism operation in the Black Sea and all merchant ships between the Ukrainian port of Odessa and the Danube's spillway into the Black Sea to move to the Istanbul Strait (Pedrozo, 2022, p. 17).

The Ukrainian ambassador in Ankara calls on Türkiye to close the Turkish Straits to military vessels belonging to the Russian Federation. On 28 February 2022, Türkiye's foreign minister, using the provisions of the Montreux Convention, announced that Türkiye was closing the straits for all warships except warships returning to ports of permanent deployment. Non-littoral states were announced not to send warships in the Black Sea (Ozberk, 2022).

As a result of this decision, NATO ship groups have also not received Turkish approval to enter the Black Sea to participate in naval exercises organized by the naval forces of the Black Sea littoral states members of the North Atlantic Alliance. In this context, the Black Sea has become a closed sea to any NATO initiative to send military vessels to the region to ensure the protection of merchant ships on the sea lines of communication. Tactical sea combat actions between the Russian Federation and Ukraine began to be conducted asymmetrically through the use of sea drift mines and unmanned systems. In order to minimize the risks of mine hazards on sea lines of communication, Romania, Bulgaria and Türkiye concluded a cooperation agreement, on 11 January 2024, on the Black Sea mine clearance through the creation of a Black Sea Mine Countermeasures Task Group (MCM Black Sea) (Dincel, Turuk, 2024).

Unmanned systems have been developed by Ukraine since the invasion of Crimea by the Russian Federation in 2014, with successful designs being manufactured in series production and delivered to the armed forces (Samus, 2024).

The concept of *asymmetric combat* was adopted by the Ukrainians as a result of the quantitative inferiority of combat forces and means compared to the capabilities of the Russian Federation. By making extensive use of unmanned systems/drones for surveillance, research, reconnaissance and attack, the Ukrainian Naval Forces have been able to effectively counter the combat power of the Russian Federation's Black Sea Fleet.

At the beginning of the conflict, in order to limit the access of Russian Federation ships to certain maritime districts, Ukrainian Naval Forces planted mine barricades along the shoreline, thus denying access to a maritime space where Ukrainian Naval Forces did not have control of the sea.

Those defensive measures were only a part of the concept of action, *"defence not being an absolute state of waiting"* (Clausewitz, 1993, p. 634), followed by attacks against Russian Federation ships with the use of littoral-ship missiles, air and sea drones on the principle *"the whole art of war consists in a well-organized defence followed by swift and daring attacks"* (Cutts, 1938, p. 21).

In the area of maritime drones, the Ukrainian Naval Forces have developed and perfected various unmanned systems that can operate at the water's surface, over considerable distances, at high speeds, equipped with explosive charges that can cause extensive damage to Russian surface vessels and even sink them. The most commonly used surface drones, Unmanned Surface Vehicle/USV, by the Ukrainian Navy or Ukrainian special services are Sea Baby and Magura V5. In order to get a picture of these unmanned naval systems it is worth mentioning that Sea Baby can develop a speed of 50 knots, approximately 90 km/h (1kt -1,852 km/h), can operate at a range of 540 nautical miles and has on board a quantity of 850 kg of explosives, while Magura V5 develops a speed of 2 knots, range of 450 nautical miles, and is equipped with 320 kg of explosives (Collective-1, 2024, p. 12).

Ukraine's combined use of Unmanned Aerial Vehicle (UAV) and Unmanned Surface Vehicle (USV) surface-to-ship missiles has significantly reduced the ability of the Russian Federation's Black Sea naval forces to utilize their capabilities in the north-western Black Sea.

The sinking in April 2022 of the destroyer *Moskva*, the flagship of the Russian Federation's Black Sea Fleet, using anti-ship missiles, marked the first resounding success of Ukrainian Naval Forces. It was followed by the sinking of a large number of Russian military vessels through repeated surface and aerial drone strikes on port facilities in Russian-occupied Crimea. The Russian Kilo-class submarine, Rostov-on-Don, was struck and sunk in the port of Sevastopol using a combination of missiles and unmanned systems (Grady, 2024). Repeated actions against naval vessels and port facilities in Crimea prompted the Russian Navy leadership to make the decision to redeploy several warships from the Russian ports of Sevastopol to the ports of Novorossiysk and Feodosia.

The execution of the strikes on Crimean port facilities has diminished the Russian Federation's ability to maintain and repair damaged warships and submarines so that the Russian Black Sea Fleet is likely to have a reduced number of naval tactical actions in the coming period. The loss of sea control in the north-western part of the Black Sea precludes the possibility of launching an amphibious assault on the Odessa region, an objective of strategic importance for both combatant countries.

Although the Russian naval blockade of the northern Black Sea has been lifted, threats to trade on sea lines of communication are still ongoing through Russian drone and missile attacks against Ukrainian grain merchant ships and Ukrainian port facilities.

The Russian Federation and Ukraine are engaged in a technological race to secure massive production of unmanned systems while improving the technology used to manufacture them in order to increase their efficiency and target effectiveness. This armed conflict has demonstrated that unmanned systems are an essential capability for shaping the operational environment due to their use in tactical actions specific to all combat environments.

The use of unmanned systems in tactical actions by the combatant sides has shaped the operational environment in the northwest Black Sea generating the following effects:

- the Russian Federation has had to redeploy its warships from the port of Sevastopol;
- the presence of Russian Federation naval vessels in the north-western part of the Black Sea has been considerably reduced;
- the possibility for the Russian Federation to carry out maritime interdiction actions on the Ukrainian coast has been reduced;
- the transportation of Ukrainian grain is affected, leading to an increase in world food prices;
- the Russian Federation is denying Ukraine access to gas and oil resources in the Black Sea;
- maritime communication lines in the north-western part of the Black Sea have become dangerous for navigation.

THE IMPACT OF THE HOUTHI REBELS' USE OF UNMANNED DRONES

As of November 2023, the Red Sea, one of the most important international cargo transportation routes from the Mediterranean Sea to the Indian Ocean, has become an unsafe maritime space for navigation as a result of repeated attacks with missiles and unmanned aerial systems executed on merchant ships by Houthi rebels. The Islamic fundamentalist movement in northern Yemen has begun launching a series of attacks using drones and rockets against merchant ships carrying goods to and from Israel. The Houthis claim that their actions are a response of solidarity with the Palestinian people and to protest Israeli military actions in Gaza (Ritter, 2024).

Amid the anti-Israel ideology, the launching of attacks on merchant ships transiting the Bab el-Mandeb Strait has disrupted shipping in the Red Sea, causing many shipping companies to abandon this trade route and choose a longer and more expensive one around the African continent via the Cape of Good Hope.

Redirecting merchant ships via the Cape of Good Hope entails an estimated 10 to 14 days longer transit, which increases transportation costs, maritime insurance, disrupts global supply and increases inflation (Economica.net, 2024).

The Red Sea is a semi-enclosed sea with a length of 1,100 nautical miles and a maximum width of 190 nautical miles. It is a shallow sea, the average depth is 490 m, about 25% is less than 50 m deep (Collective-2, 2024, p. 1). The Red Sea is connected to the Mediterranean Sea through the Suez Canal and the Indian Ocean through the Bab el Mandeb Strait, being the most important line of communication linking Europe to the Middle East and Asia. The Bab el Mandeb Strait is a narrow strait between 26-32 km wide and 112 km long and is the key to controlling shipping between Europe and Asia. The International Maritime Organization/IMO estimates that about 25% of global seaborne cargoes pass through this route, mainly crude oil and petroleum products from the Persian Gulf to Europe.

The geostrategic position of the Red Sea provides the Houthi rebels with maritime space where they can carry out missile and unmanned missile system attacks against merchant ships, creating a security crisis in the region, with the aim of promoting their Islamic revolution, anti-Israel, anti-American ideology, and to control the region by destabilizing the security environment.

In response to attacks by Houthi rebels, naval forces belonging to the United States of America and Great Britain have been deployed in the Red Sea. The US Navy has been executing response actions in self-defence since December 2023 following an attack by Houthi rebels on a merchant vessel.

On 18 December 2023, US Secretary of State, Lloyd Austin, announced the formation of a coalition of 20 states and the launch of Operation *Prosperity Guardian* to protect merchant ships transiting the Red Sea. Operation *Prosperity Guardian* brings together several countries such as the USA, UK, Canada, Bahrain, Italy, the Netherlands, Norway, Seychelles, Spain to address the challenges of the Red Sea security environment in order to ensure freedom of navigation in the Red Sea for all merchant vessels and enhance regional security and prosperity (Defense Romania, 2023).

The European Union, on 29.01.2024, took steps to launch an operation in the Red Sea, *EUNAVFOR ASPIDES*, in close cooperation with the coalition maritime operation *Prosperity Guardian*, with the aim of protecting maritime security on the main shipping lanes in the Bab el Mandeb Strait, the Strait of Hormuz, the international waters of the Red Sea, the Arabian Sea and the Persian Gulf. Operation *EUNAVFOR ASPIDES* was launched on 19 February 2024, on the occasion of the meeting

of the Foreign Affairs Council of the European Union (Agerpres, 2024). Romania has committed to contributing to the coalition maritime operation *Prosperity Guardian*, with staff officers, within the command deployed on the territory of Bahrain, after the legal status of Romanian military personnel on the territory of this state is settled (Juridice.ro, 2024).

The attacks by Houthi rebels on maritime lines of communication in the Red Sea have prompted a collective effort by the international community to support freedom of navigation and eliminate the danger posed by the use of ballistic missiles and unmanned aerial and naval systems. The actions of the Houthi rebels are designed to provoke a strong response from regional actors and those with economic interests in the region, internationalizing the conflict by challenging the influence of the United States of America and Israel in the region. By escalating the conflict, the Houthi rebels are convinced that they have little to lose, relying on their resilience and adaptability to military pressure and the military support they receive from Iran. The Houthi leader, Abdul-Malek al Houthi, has stated that they are prepared for the introduction of unmanned underwater systems, which entails a strategic shift aimed at improving their ability to strike commercial and military vessels in the Red Sea (Feierstein, Alasrar, 2024).

The use by Houthi rebels of unmanned systems in their actions against merchant ships in transit through the Red Sea has generated a number of effects with economic and military impact as follows:

- the disruption of shipping through the Red Sea with immediate effect on global supplies, increased prices of commercial goods and maritime insurance;
- significant military, financial and diplomatic efforts by the international community to maintain freedom of navigation in the Red Sea by forming a coalition and launching Operation *Prosperity Guardian*;
- the launch by the European Union of Operation *EUNAVFOR ASPIDES*, with the aim of protecting the maritime security of the Red Sea lines of communication;
- the escalation of the conflict in the Middle East region, which requires the maintenance of a considerable military presence in the region and, therefore, special financial efforts.

The effects of the use of ballistic missiles and unmanned systems by the Houthi rebels are not only economic, but also political and social. The strategic calculus now involves not only a military response but also diplomatic efforts to maintain regional

stability. The implementation of the decisions of international organizations to sanction Houthi supporters can stop the flow of weapons and advanced technology to the Houthi rebels, and thus it would become possible to reduce attacks and intercept the vectors launched at commercial ships.

CONCLUSIONS

The extremely dynamic development of modern technologies has influenced many fields of activity, with drones/unmanned systems becoming a key sector for research and deployment of artificial intelligence.

An important area for the use of new developments in innovative technologies and research remains the military segment. The war in Ukraine and the conflict in the Red Sea highlight the importance of globalization and the development of modern technologies.

Unmanned systems are likely to play a decisive role in the warfare of the future in order to achieve success and conduct military actions in all combat environments. This statement is supported by the main characteristics of unmanned systems:

- Unmanned systems prove their efficiency through their simplicity of construction and the multitude of missions for which they can be configured;
- Mission complexity is directly proportional to the degree of technological development;
- Multi-functional unmanned systems allow easy adaptation of the equipment to the recipient's requirements, while retaining the freedom to introduce new innovations to improve efficiency and increase range of travel.

Enclosed and semi-enclosed seas are the ideal place where unmanned systems can operate with high efficiency, due to the small distances between targets and the possibility to operate from multiple directions.

One of the great advantages of using unmanned systems in confined maritime spaces is the flexibility to use multirole capabilities.

Unmanned systems can be configured for a variety of missions such as:

- naval surveillance;
- vessel traffic monitoring;
- search and rescue;
- direct action against commercial or military vessels.

In the future, it is possible that fleets of autonomous merchant ships will be sailing on the maritime communication lines, which will open a new chapter in the field of maritime transportation and also in the military field. Thus, the safe transit

of merchant ships on the sea lines of communication can be ensured by unmanned military naval systems, thus eliminating the exposure of the human factor to various dangers generated by the changing security environment.

Unmanned systems will probably not solve all situations generated by an armed conflict, but they can contribute effectively in several areas to gaining advantages over the enemy.

BIBLIOGRAPHY:

1. Agerpres (2024), https://www.agerpres.ro/viata-parlamentara/2024/04/22/parlamentul-a-aprobat-scrisoarea-presedintelui-privind-participarea-armatei-la-eunavfor-aspides-si-solicitarea-de-a-participa-la-prosperity-guardian-1284845, retrieved on 22 June 2024.
2. Ciorobea, C. (2024). In *GeoPolitica*, https://www.geopolitic.ro/2024/02/strategia-de-securitate-sua-la-marea-neagra-implicatii-regionale/, retrieved on 12 May 2024.
3. Clausewitz, von C. (1993). On War, Michael Howard, Peter Paret (eds., translators), New York.
4. Collective-1 (2024) (Midttun Hans Petter, Frolova Alina, Klymenko Andrii, Ryzhenko Andrii). *The impact of Ukraine's asymmetric approach on Russian Sea Power in the Black Sea*. Kyiv.
5. Collective-2 (2024) (Najeb M.A. Rasul, Ian C.F. Stewart, Zohair A. Nawab). *Introduction to the Red Sea: Its Origin, Structure and Environment*, https://www.researchgate.net/publication/291002173_Introduction_to_the_Red_Sea_Its_Origin_Structure_and_Environment/link/669899634a172d2988aa2c02/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19, retrieved on 22 May 2024.
6. Cutts, F.E. (1938). *Operation for Securing Command of the Sea Areas, Newport*. Naval War College.
7. Defense Romania (2023), https://www.defenseromania.ro/coalitia-maritima-din-marea-rosie-operatiunea-prosperity-guardian-impotriva-rebelilor-houthi-este-iminenta_626071.html., retrieved on 22 May 2024.
8. Dincel, S., Turuk, U. (2024), https://www.aa.com.tr/en/europe/turkiye-romania-and-bulgaria-establish-task-force-to-demine-black-sea/3263294, retrieved on 12 June 2024.
9. Economica.net, AGEPRES, 2024, https://www.economica.net/conflictul-din-marea-rosie-nu-inseamna-o-noua-criza-a-lanturilor-de-aprovizionare-analiza_720406.html., retrieved on 23 May 2024.
10. Feierstein, G.M., Alasrar, F.A. (2024). *The Middle East Institute*, https://www.mei.edu/publications/geopolitical-implications-houthi-attacks-and-israeli-retaliation, retrieved on 22 May 2024.
11. Grady, J. (2024). USNI News, https://news.usni.org/2024/08/04/russian-attack-submarine-sunk-in-missile-strike-on-black-sea-port-claims-ukraine, retrieved on 23 May 2024.

12. Hanganu, M. (1998). *Apărarea comunicaţiilor maritime de către forţele flotei maritime în condiţiile geopolitice actuale*, in *Gândirea militară românească*, no. 1.
13. Itinerarii pontice/Marea Neagră, https://ecomareaneagra.wordpress.com/marea-neagra/, retrieved on 2 August 2024.
14. Juridice.ro (2024), https://www.juridice.ro/734157/armata-romaniei-participa-la-operatia-maritima-de-tip-coalitie-prosperity-guardian-opg.html., retrieved on 18 June 2024.
15. Moraru, E.G. (2011). *Regimul juridic al navigației în Marea Neagră și situația Strâmtorilor Bosfor și Dardanele*. București.
16. Nistor, F., dr., Scipanov, L.V., dr. ing. (2021), *Influența caracteristicilor Mării Negre asupra operațiilor întrunite*, in *Impact Strategic*, București, no. 3.
17. Ozberk, T. (2022). *Naval News*, https://www.navalnews.com/naval-news/2022/02/turkey-closes-the-dardanelles-and-bosphorus-to-warships/, retrieved on 22 May 2024.
18. Pedrozo, R. (2023). *The Russia- Ukraine Conflict: The War at Sea*.
19. Ritter, S. (2024). *Consequence of the Houthi Attack, Energy Intelligence*, https://www.energyintel.com/0000018d-1c3a-db4a-a9cf-fe7b997d0000, retrieved on 22 May 2024.
20. Samus, M. (2024). *Lessons learned from the war in Ukraine. The impact of drones*, https://newstrategycenter.ro/wp-content/uploads/2024/02/Lessons-Learned-from-the-War-in-Ukraine.-The-impact-of-Drones-2.pdf., retrieved on 22 May 2024.
21. Till, G. (2013). *A Guide for the Twenty-first Century*, 3rd ed. Routledge, London and New York.
22. UNCLOS, United Nations, Art. 122, %20https://www.un.org/Depts/los/convention_agreements/texts/unclos/unclos_e.pdf%20, https://www.un.org/Depts/los/convention_agreements/texts/unclos/unclos_e.pdf, retrieved on 22 May 2024.
23. Vego, M. (2007). *Joint Operation in the littorals: Doing more with less*, Military Database.
24. Vego, M. (2017). *Maritime Strategy and Sea Control, Theory and Practice*, https://defence.org.ua/wp-content/uploads/The-impact-of-Ukraine%E2%80%99s-asymmetric-approach-on-russian-sea-power-in-the-black-sea.pdf., retrieved on 22 May 2024.
25. Vespremeanu, E. (2005). *Geografia Mării Negre*. București: Editura Universitară.

INTEGRATION OF FIRST PERSON VIEW (FPV) UNMANNED AERIAL SYSTEMS IN ROMANIAN GROUND FORCES OPERATIONS

Lieutenant Colonel Senior Instructor George-Ion TOROI, PhD

"Carol I" National Defence University, Bucharest

DOI: 10.55535/RMT.2024.4.08

The war in Ukraine is an inexhaustible source of operational lessons for the armed forces. Against the backdrop of the growing operational use of unmanned aerial systems (UAS), this article discusses the potential of integrating FPV systems into the Romanian Armed Forces' ground operations and provides a comprehensive analysis of the potential benefits of such a decision.

Against the background of the need to integrate emerging technologies in the process of force structure adaptation, the study provides arguments in favour of acquiring such a combat technology, based on the experience of the two belligerents in the Ukraine conflict, but also of other actors who have already decided to implement these systems in their own force structure.

In addition, the paper provides a combat functional analysis of the operational use of FPV drones, highlighting the advantages and challenges of this technology in the current military context, as well as potential evolutionary trends. The study concludes that the integration of these systems in the armed forces can bring several tactical advantages, but it is essential that this decision should be well-founded and take into account the specific context and requirements of the Romanian Armed Forces.

Keywords: drone; UAS; strike system; Ukraine conflict; FPV;

Motto:

"The development of drone technology has forever changed the landscape of warfare".

Barack Obama

INTRODUCTION

Beyond the destructive nature inherent in any armed conflict, the war in Ukraine is an inexhaustible source of operational lessons that should be fully exploited in the process of adapting the armed structures and the ways of conducting military operations. In more than two and a half years since the conflict began, it has provided countless lessons.

First, the challenges of force protection have become extremely complex against the backdrop of an increasingly transparent operating environment, brought about by technological developments in surveillance and data collection capabilities, but also by the expansion of long-range precision strike capabilities. These developments have led to the need to adapt military doctrine and practice to meet new threats and challenges.

Decentralising command and control and disposition of forces for their protection is one way of adapting armed operations to the specific challenges and threats of today's confrontational environment. The ongoing conflict in Ukraine has also demonstrated the paramount importance of sustainability. In a conflict of attrition such as this, the ability to ensure long-term logistical support makes the difference between success and failure. It has been crucial in the development of the conflict in Ukraine.

But perhaps the most important lesson at the tactical level is the automatization of the battlespace, with direct implications for the conduct of ground operations. Unmanned aerial systems (UAS) have become a central element of the modern battlefield and are changing the character of conflicts in all domains and at all levels.

Since the beginning of the conflict in Ukraine, these systems have brought about a significant metamorphosis in the paradigms of ground combat. While they also proved their effectiveness in the Nagorno-Karabakh conflict between Azerbaijan and Armenia, where they were described as magic bullets (Hambling, 2020) due to their devastating impact on traditional enemy technology and operations, the Russian-Ukrainian war has led to a significant evolutionary leap in the use of UAS

in support of land forces operations. These systems have had a major impact on the way battles are fought, completely changing the dynamics of the conflict and directly influencing the tactics employed by both sides. Some authors refer to the conflict in Ukraine as the *"drone war"*. (Gosselin-Malo, 2024). Moreover, the role of UAS systems in armed conflicts is expected to increase as the technology continues to evolve, leading to an urgent adaptation of the specific military doctrines of NATO countries (Borsari, 2023, p. 3).

In Ukraine, these systems have proven their effectiveness in surveying the battlefield and providing real-time intelligence for rapid engagement of detected targets. They have also proven their usefulness in neutralising threats by conducting direct strikes on enemy targets. In this landscape, UAVs have been not only an asset for both sides in gaining operational advantages over the adversary, but also a significant challenge in maintaining high operational capability by protecting forces, operations and assets. *"The use of unmanned aerial systems has created a transparent battlefield where there is no hiding place"* (Collins, 2023, p. 8).

Although the two-and-a-half-year conflict has seen a number of adjustments in the use of drones, their role has grown exponentially. From the successful use of the Turkish-made Bayraktar TB2 by the Ukrainians in the early stages of the conflict, to the use of commercial drones such as the DJI modified for reconnaissance and precision strikes, to the integration of kamikaze drones and loitering munitions such as the Switchblade and Shahed, the war in Ukraine has seen a continuous adaptation of UAS systems and their operational use to secure tactical advantage. The Russian-Ukrainian conflict is the first in which commercial drones have been used alongside military drones on a large scale and with significant impact.

Currently, the most widely used UAS systems in the Russian-Ukrainian conflict are FPV (First Person View) (Milasauskas, 2024). They are considered the latest evolution of UAS systems, as demonstrated by both the conflict in Ukraine and the conflict between Israel and Hamas (Operational Environment 2024-2034: Large-Scale Combat Operations, 2024, p. 11). FPV drones are types of aerial platforms equipped with cameras and video transmission systems that provide real-time video data to a ground console controlled by an operator. Their main advantage is their extremely low price compared to others (Borsari, 2023, p. 14). The primary use of these systems is to attack the opponent's capabilities in the contact zone, with both combatants using these drones extensively and successfully.

However, despite their proven operational effectiveness in the Russian-Ukrainian conflict, the Romanian Army does not currently have a plan to acquire and equip its ground structures with such systems (Barbu, 2024, pp. 11-13). This is the *research*

problem from which this scientific endeavour is initiated. In relation to it, *the main research objective* of this study is to bring to the attention of the decision- makers of the Romanian Army the need to consider FPV drones for their acquisition and use in military operations in order to optimize the response to the challenges of the current operating environment.

The research methodology used is qualitative, seeking to understand the nuances of the operational use of FPV drones and to argue the need for it in the context of the specific approaches to the conflict in Ukraine. Accordingly, the argumentation is inductive, drawing general conclusions from systematically collected and analysed data. The main target of the study is represented by the decision-making structures of the Romanian Army, and the results obtained provide solid arguments for the integration of FPV UAS systems into the ground force structures.

Considering the qualitative nature of the study, *the research questions* that have guided the approach to the problem, in order to achieve the aforementioned objective, are as follows:

❖ *What are the characteristics of FPV drones and how can they be interpreted from a military point of view?*

❖ *How have FPV UAS systems been used in the conflict in Ukraine?*

❖ *What are the advantages of using such systems in military operations from a warfighting perspective?*

❖ *What is the approach of international actors to the use of FPV drones in military operations?*

Based on the analysis of secondary data from unclassified open-sources, we have structured this paper in two parts. In the first part, we have provided a military interpretation of the specific design and functional characteristics of FPV drones. In the second part, we have tried to provide answers to the last three research questions. Thus, we have presented and interpreted different examples of the use of these systems in the Russian-Ukrainian conflict, made a functional analysis of their operational use in military operations, and identified different approaches of international actors to this issue.

FPV DRONES – TECHNOLOGY AND FEATURES

Unmanned aerial systems are a complex mechanism that includes both the aircraft and the support network, equipment and personnel required to control it (Joint Doctrine Publication 0-01.1 UK Terminology Supplement to NATO Term, 2023, p. 59; FM 1-02.1 Operational Terms, 2024, p. 80; AAP-06, 2021, p. 134).

In addition to military drones, commercial drones have played an extremely important role in the conflict in Ukraine. The latter have developed steadily over the past two decades. A report last year estimated the value of commercial drone transactions worldwide at around $30.6 billion, with an estimated increase to around $55.8 billion by 2030 (Anwar, 2023).

Even if their capabilities are inferior to military ones in terms of speed, payload, range or sensor quality, and they are more vulnerable to electronic warfare (EW) systems, the conflict in Ukraine has demonstrated their importance and effectiveness in intelligence, surveillance and reconnaissance (ISR) or even target engagement missions. Their much lower cost, ease of access and the need to find solutions to enhance the operational capabilities of ground forces have made commercial drones an indispensable element of contemporary conflict. Their creative exploitation in the Russian-Ukrainian war involved a significant change in the way ground operations were conducted.

A highly effective UAS system in this conflict is represented by FPV (First Person View) drones, which are also the most widely used by both combatants (Milasauskas, 2024). Originally built for entertainment purposes for competitions, they have become a constant in current actions by both Ukrainians and Russians. They are a crucial tool for data collection and target engagement. This section will provide a military analysis of the specific characteristics of this type of system to explore how they can be integrated into combat operations.

It is important to note that the FPV airborne system involves more than just aircraft. For it to work optimally, it also requires specialised personnel to operate it, as well as a control station and VR (virtual reality) goggles. It is also important that the drone has a high-performance video camera for effective terrain monitoring, and a communication link with the control station to operate the drone according to the situation. *Figure 1* highlights the main components of an FPV drone ready for target engagement.

Unlike the other types of commercial drones that have been widely used in Ukraine, where the image the drone records is found on the drone's controller, FPV drones require a set of VR goggles, which makes the experience much more realistic. It is as if the operator is on board the aircraft. This allows the pilot to see what the drone is seeing in real time, giving a bird's eye view of the battlespace and a much greater degree of control.

FPV drones are also equipped with high-resolution cameras that transmit clear and detailed images to the pilot, allowing him or her to have full control

of the mission. What is more, these cameras can also be deployed at night which can ensure the ability to monitor the battlefield 24 hours a day.

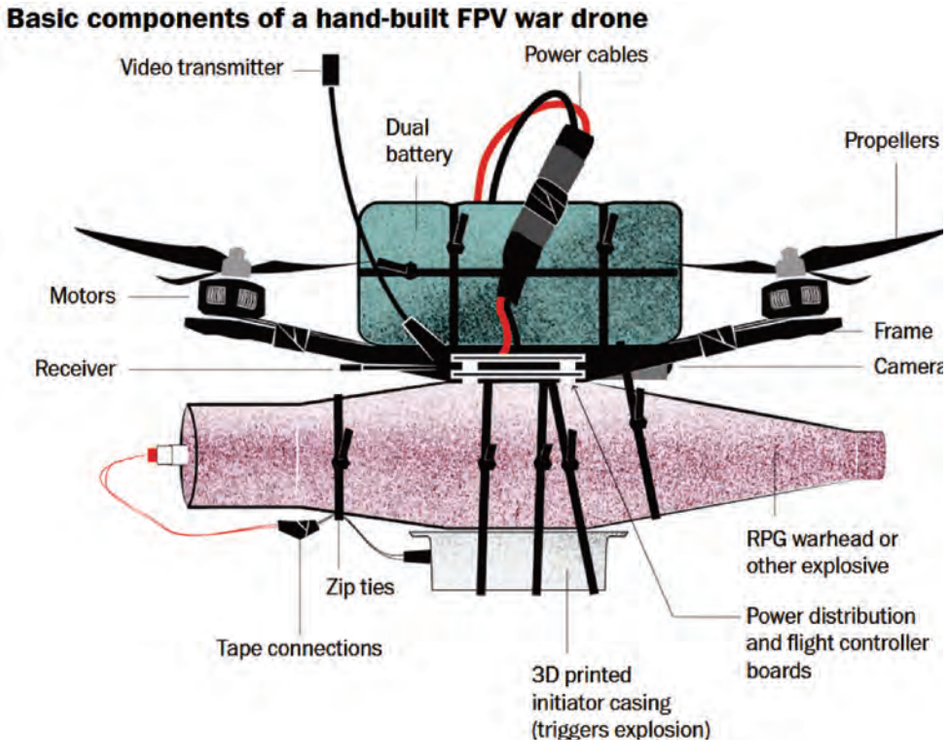


Figure 1: *Component parts of an FPV drone configured for target engagement* (Horton, 2023)

Moreover, they are equipped with advanced stabilization and navigation technologies that increase accuracy, they can hit targets even through tank hatches or the narrow windows of buildings specific to urban combat (Milasauskas, ib.), and are much more manoeuvrable than other types of commercial drones. FPV drones can also be used to destroy optical devices, radars or antennas mounted on the exterior of military vehicles (Ib.), which further demonstrates their effectiveness.

However, because they are operated by humans, the operator's ability to precisely manoeuvre FPV drones is crucial to achieving results. They are the brain of the drone. It is therefore extremely important that they are well trained in order to maximise the potential of these systems. FPV drones require much more skill to operate than other commercial drones. It takes at least two to three weeks to master the skills required to operate such a drone. In addition, operators must undergo certain special medical tests. For example, reaction speed, finger dexterity

or the vestibular system are checked to understand how well the operator is prepared to deal with stress and pressure situations during operations (FPV Drone Control: Exploring Effectiveness and Risks in Military Operations in Ukraine, 2023). All of these imply limitations in terms of identifying and training personnel who can operate such systems.

The most important specifications of FPV drones relevant for combat use are related to the degree of flight autonomy, travel speed or payload capacity. Flight autonomy is dependent on battery autonomy. Most commercial FPV drone batteries have an autonomy of between 5 and 10 minutes.

The higher speed of up to 250 km/h compared to other types of commercial drones, while requiring a higher degree of operator skill, ensures that the enemy's main kinetic measures and electronic jamming systems can be avoided (Rhodes, 2024, p. 11). Destruction by infantry strikes with small calibre weapons is the second most common means of destruction of commercial UAS. The higher speed, combined with the small size of the drone, gives FPV drones a greater chance of survival than the others (Ib., p. 1).

Speeds of up to 250 km/h and battery autonomy mean that the range can be up to 10 km. In military terms, it would mean that it could cover roughly the depth of an enemy's 1st echelon manoeuvre battalion. Therefore, the applicability of FPV UAS systems is in contact, with the potential to affect the enemy's operational capability in this area. The installation of additional batteries, as well as the use of relay drones, has ensured that the Ukrainians are able to extend the range of the kamikaze drones to 10-20 km (How Ukraine's cheap FPV drones are used on the Ukrainian battlefield, 2023), thus having the possibility of attacking the weapon reserves and command points of the enemy's 1st echelon brigades.

In addition, the quality of the integrated video camera, the resistance to extreme weather conditions and the security level of the control system must also be taken into account.

Navigation capabilities such as GPS and obstacle avoidance can also make a difference in military operations.

To ensure effective communication between the drone and the operator, the characteristics of the transmission module and the range of the system are also important.

Given their primary military role, that of target engagement, the payload capacity of FPV drones is an extremely important feature, as it determines the type of munitions they can carry and, consequently, the types of targets they can engage and destroy. Most can carry up to one kilogram of extra weight,

but there are some that are more capable, such as the Ukrainian Skynight, which can carry a payload of up to 2.5 kilograms (McFadden, 2023). In addition, a video presentation highlights that the Ukrainian military has equipped itself with a type of FPV drone capable of carrying a projectile of up to 5 kilograms, significantly increasing its target destruction potential. It was achieved by adding 2 extra engines (6 in total), but it also increased the size of the aircraft. The purpose of this drone would be to destroy buildings and fortifications in which the enemy is hiding in order to facilitate access for smaller drones (Ukrainian new heavy FPV drones with enhanced warheads will be *"nightmare"* for Russians, 2024).

The biggest advantage of an FPV drone is its price. Even the best models cost half as much as a Mavik (Borsari, 2023, p. 14). Thus, the conflict in Ukraine has demonstrated time and again how an FPV drone, whose price starts at $500, can carry a payload that can hit an enemy tank costing several million dollars. Even though the lifetime of FPV UAS systems is days due to their vulnerability to jamming and small arms attacks, the use of a large number of such low-cost commercial drones is financially and operationally cost-effective, compensating for these shortcomings and providing significant tactical advantages, as demonstrated in the Ukraine conflict.

But the main disadvantage of these and other civilian drones is that they are vulnerable to electronic warfare. This is considered to be their Achilles heel. However, the systems have proven to be more resilient to electronic jamming than other commercial systems and can adapt effectively to enemy tactics. The ability to adjust control frequencies, transmit images over a wider range, or receive both digital and analogue types of video transmission make FPV UAS systems more resilient to electronic jamming (Milasauskas, ib.; FPV Drone Control: Exploring Effectiveness and Risks in Military Operations in Ukraine, 2023). Even though they present a certain vulnerability to EW (electronic warfare) systems, few actors can afford to cover the entire front with such devices. In addition, electronic jamming involves emitting a signal that is stronger than the one being jammed, which requires fairly powerful and bulky equipment that is not always feasible for contact manoeuvre units. Furthermore, their use would make EW equipment vulnerable to subsequent attack by their own forces. So, even when not carrying out their strike mission, FPV drones can be used as decoys to create vulnerabilities for the enemy. In addition, recent innovations in areas such as customised frequencies, frequency hopping and automated flight patterns promise to further enhance their effectiveness.

However, FPV technology is critical to the way modern operations are conducted, as evidenced by its extension to other types of platforms, such as unmanned ground

vehicles (UGVs), with Russia already developing such FPV ground kamikaze systems (Russia Produces a Series of Ground FPV *"Kamikaze"* Drones, 2024).

Next, in relation to the military characteristics and interpretations provided above, we proceeded to conduct a SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis to objectively assess the appropriateness of integrating FPV systems into military organizations. To ensure a higher degree of fidelity of the results obtained, for each element identified in the SWOT analysis, we also performed a military inference to provide a clearer perspective on the benefits and risks of integrating these systems into operational practice. *Table 1* presents the result of this analysis process.

Table 1: SWOT analysis on FPV UAS systems (author's design)

Strengths	Weaknesses
• **Low cost** – ability to purchase and operate a relatively large number of drones; • **High manoeuvrability** – increased efficiency compared to other commercial drones; • **Operational versatility** – can perform a wide range of missions; • **Small size and high speed** – can provide greater protection against enemy destructive actions; • **Real-time control** – can ensure timely decision making.	• **Limited autonomy** – range limitations; • **Relatively small payload but larger than most commercial UAS** – can successfully engage only certain types of targets; • **Vulnerability to electronic jamming** – technological advancement may ensure its limitation; • **Lacks its own systems to protect against enemy attack** – operator dexterity is the only way to avoid it; • **Dependent on weather conditions.**
Opportunities	**Threats**
• **Technological development –** increasing carrier capacity, range, protection against electronic jamming threats or integrating artificial intelligence to create drone swarms; • **Integrated use with other weapons systems –** making joint warfare more effective.	• **Electronic countermeasures** – vulnerability to electronic jamming; • **Evolution of enemy protection systems.**

ARGUMENTS FOR THE NEED TO INTEGRATE FPV DRONES INTO ROMANIAN ARMY GROUND OPERATIONS

Operational Use of FPV UAS in the Russian-Ukrainian Conflict

Ukraine's extensive use of unmanned aerial systems has demonstrated their effectiveness in gaining tactical advantages against a far superior adversary such as Russia (Borsari, p. 7). Both sides have used these types of systems to remarkable effect for ISR missions, for correcting artillery fire, BDA (Battle Damage Assessment), or for hitting targets by improvising them as kamikaze weapons (Borsari, p. 13). The impact of these systems has been extremely high in this conflict and it is expected to increase, comparable to that of the machine gun in the First World War.

FPV drones have proven to be among the most frequently used weapons in the Ukrainian conflict, where one of the belligerents was unable to gain air superiority due to the overstretch and high efficiency of anti-aircraft systems (Zafra, 2024). It is also due to their increased efficiency relative to the purchase price. The success rate of FPV-type UAS systems in the conflict in Ukraine is estimated to be between 50% and 80% (How could FPV drones change warfare?, 2023). Moreover, some analyses of the use of such systems in the Russian-Ukrainian conflict show a trend towards their increasing use as a means of striking various targets, as can be seen in *figure 2*.

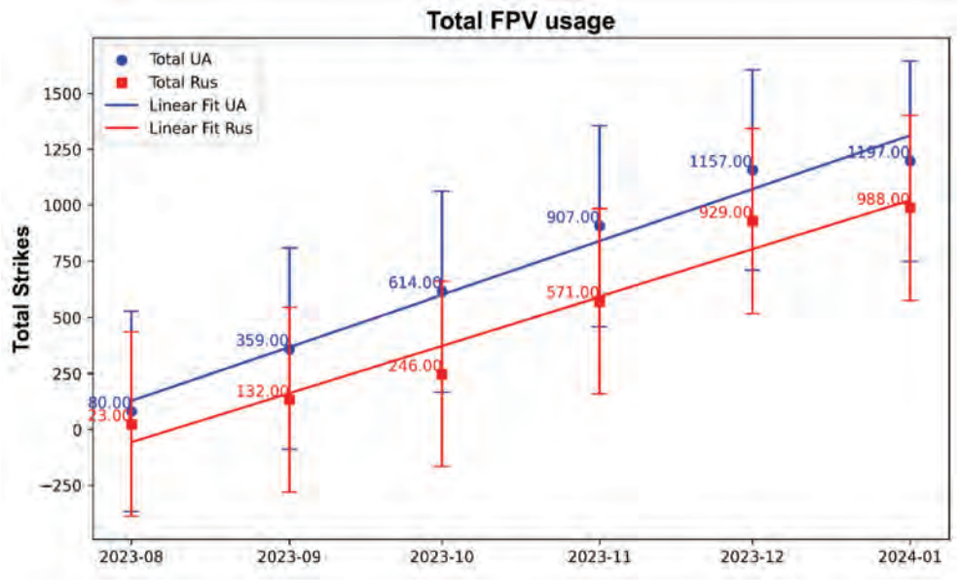


Figure 2: Using FPV drones in the Russian-Ukrainian conflict (Ben, 2024)

Given the complexity of the situation in Ukraine, we believe that it is essential to focus our attention first and foremost on the operational lessons learned from the use of FPV drones in this conflict, in order to implement more effective resource management strategies during military operations, as well as to optimize our own approach to the use of this technology in a military context. We appreciate that such an approach will provide the framework for the Romanian Army to better adapt to the way FPV drones are used in military operations. Furthermore, highlighting the efficiency of the use of FPV UAS systems will contribute to the understanding of the operational need for such aircraft in order to strengthen the Romanian Army's capabilities in the face of the increasingly diverse threats in the current security environment.

There are numerous examples of the use of FPV drones in the Russian-Ukrainian conflict. The analysis conducted presents an approach to how they have been used in different operational contexts in order to understand their versatility and effectiveness in deployed operations.

As noted above, the effectiveness of these types of devices is reflected in the area of contact. Therefore, the targets engaged are those found here. The most common use of these drones is to destroy armoured vehicles, mortars, artillery equipment and artillery because they are equipped with anti-tank missiles (A Drone Worth a Few Hundreds of Dollars against a 240-mm Mortar: Spectacular Destruction of the Tyulpan Mortar at a Distance of 10 km, 2023). Their effectiveness is also proven by the fact that even the most advanced Russian tanks, the T-90 Proryv, have fallen prey to FPV UAS attacks ('$500 – Ukrainian drone, $3 million –Russia's most advanced tank, a skilled operator's hands – priceless', 2024).

They can therefore be used against a wide range of enemy technology, stationary or mobile, such as artillery systems, tanks, armoured fighting vehicles, as well as command posts or observation posts. It should be noted that FPV drones can even engage personnel dug in trenches, an effect that is difficult to achieve with direct-fire weapons (Ukrainian FPV kamikaze drones attack Russian military equipment, 2023).

The Ukrainian military has recently adopted a new way of using FPV drones, equipping them with thermite. Mainly used in metallurgy or welding, thermite is a mixture of aluminium and iron oxide that, when ignited, burns with high heat release (DEX online, 2024), about 2,500 degrees Celsius, enough to corrode iron in seconds. Placing a charge of about 500 g under the drone can have a devastating effect on the enemy. The chemical reaction can be initiated by remote control when the aircraft is near the target area. The Ukrainians have successfully used

such a method, called *Dragon Drone*, to destroy an enemy hiding in wooded areas (What are 'dragon drones', Ukraine's latest weapon against Russia?, 2024).

FPV drones are also believed to have been used by the Ukrainians to destroy much more valuable targets. The destruction of a Russian Mi-24 attack helicopter in August this year in the Kursk region (Ukrainian FPV Drone Rams Russian Mi-24 Helicopter, 2024) or of a rather powerful Murom-P surveillance system (Ukrainian Military Destroyed Russian Murom-P Surveillance System Once Again, 2023), capable of detecting people and vehicles at a range of almost 10 km, are just two of the most high-profile examples.

In addition, the Russian-Ukrainian war has demonstrated a continuous adaptation of how FPV UAS systems can be used. Recently, drone-on-drone engagements have been recorded, demonstrating that these systems are following an evolution similar to that of aircraft in the First World War, when they were first used for reconnaissance, then for fires, and finally for confrontation (Ukrainian MoD highlights 'drone-on-drone' engagements over the battlefront, 2024).

Analysis of the Use of FPV UAS from the Perspective of Combat Functions

It is easy to see the significant role these systems are playing in the ongoing conflict in Ukraine. While the primary mission of FPV drones is to engage targets in the contact zone, these systems can support the performance of multiple combat functions and are perhaps the most versatile capability in the arsenals of both belligerents.

For example, from a **command-and-control** perspective, these capabilities can provide commanders in the contact zone with a greater degree of real-time situational awareness. Moreover, the presence of such capabilities at lower hierarchical levels (battalion/brigade) can support freedom of action and decentralization of command, critical elements of an effective C2 system, as demonstrated in the Russian-Ukrainian conflict. It can thus streamline decision-making and quickly exploit fleeting opportunities as events unfold. In addition, such a capability can support command and control by ensuring more effective coordination of subordinates' actions during difficult moments in the battle. Furthermore, depending on the situation, drones can also act as relays to ensure communication with different structures, thus contributing to their command-and-control capability.

Although, as mentioned above, the main mission of FPV UAS systems is to strike, thanks to the high-performance video camera they can also be used in research and surveillance missions, ensuring the monitoring of the confrontation space, both day and night. The continuous collection of information in real time ensures

a better understanding of the operational situation. These systems can also support the targeting process by identifying targets or ensuring the adjustment of artillery systems. They can also support the Battle Damage Assessment (BDA) process. These are all essential elements of the **intelligence** function.

FPV-type UAS systems can provide firing **manoeuvre** according to the operational situation. They can also support the investigation of troop movement routes to support troop manoeuvre. In addition, they can be used to cover flanks and open gaps between units, provide **force protection**, and monitor their own **logistical** supply lines.

However, the conflict in Ukraine has demonstrated that the two most important combat functions that FPV UAS systems can support are **fire support and reconnaissance**.

As the Russian-Ukrainian conflict has demonstrated, the operational importance of FPV drones is extremely high in terms of engaging a wide variety of targets, as described in the previous section. By equipping them with various munitions, the systems have become formidable precision weapons, capable of providing significant advantages to the user and corresponding negative effects to the adversary. The engagement procedure is simple and consists of three steps:

- *Target identification.* It can be accomplished through proprietary information gathering systems that provide coordinates and an image of the target.
- *Engagement planning.* Once accepted, the target must be approved and the type of engagement (artillery, FPV etc.) selected. In the case of FPV UAS, it is also necessary to select the type of payload specific to the effect to be achieved, define the route and deconfliction with other UAS already on the route, and establish the communication channel with the aircraft.
- *Execution.* The operator receiving the mission manoeuvres the drone to the received coordinates along the specified route, while also performing terrain reconnaissance along the route. He then detects the target and determines how to engage it to achieve the desired effect. It is very important that the operator is extremely well trained, both in handling the drone and in knowing how to exploit the vulnerabilities of the target he is engaging.

It can therefore be seen that in order to operate effectively, the UAS must be manned by a team to approve the target, prepare the payload and aircraft for operation, and pilot it to the engagement area.

Additionally, thanks to the performative camera, all of these successes in neutralizing certain capabilities of the adversary can be recorded and used to influence target audiences, as we can observe almost every day on social media

platforms (Jones, 2023, pp. 21-22). In a conflict for gaining information superiority, this method becomes a crucial one.

One can therefore see the high degree of versatility in the operational employability of FPV UAS systems, as they support numerous combat functions, depending on the context.

The Importance Given by Different International Actors to FPV UAS Systems

First, the importance of FPV UAS is demonstrated by the actions taken by the two belligerents in the Russian-Ukrainian conflict. **Russia** is actively developing FPV drones. One example is the Chinese-made *"Boomerang"* drones, which, even though they use cheap manufacturing materials, are quite efficient (Russia's Boomerang Copter-Class Small FPV Drones, 2023). Due to their affordability and importance, FPV technology has also been deployed by Russia on unmanned ground platforms (Russia Produces a Series of Ground FPV 'Kamikaze' Drones, 2024). It is recognized by Russian specialists that *"the future belongs to compact and agile, short-range FPV drones used at platoon level for reconnaissance and precise strikes"* (Edmonds, 2023).

In addition, Russia has increased production of FPV drones. In April of this year, the country's president announced plans to invest $1 billion by 2026 to develop and purchase such drones, and about $2.2 billion by 2030 (Putin wants "mass production" of drones in Russia, 2024). These significant investments demonstrate the importance Russia attaches to the development and purchase of FPV UAS systems amid the effects of these drones in the conflict in Ukraine. At the end of July 2024, Russian Defence Minister Andrei Belousov announced a production of about 4,000 FPV drones per day for his country, which means about 1.5 million units per year (How Realistic Are Russia's Statements about Production of 4,000 FPV-Drones Per Day?, 2024). In addition, the Russian Federation also recognizes the need for operator training. A Russian report from earlier this year highlights that Russia had trained about 3,500 operators in more than 800 special training facilities so far (3,500 Drone Operators Trained in Russia, Ministry of Defence Claims, 2024). These figures reflect the scale of Russia's investment in this type of weaponry; while demonstrating the importance it has attached to it in the wake of developments in the Ukraine conflict.

In addition, Russia is increasingly focusing on research in this area in order to increase its effectiveness. An extremely important example in this regard dates back to the beginning of the year, when Russian media reported on the development of a Russian FPV drone carrier. It is extremely significant, as it can extend the range of the systems, within the maximum signal limit, to engage targets deep inside

the Ukrainian device (https://www.defensemirror.com/news/36386/Russia_Tests_FPV_Drone_Carrier_in_Ukraine, 2024). The installation of retranslation stations on some of the drones, filters blocking certain frequencies to increase resistance to enemy electronic jamming systems, or the use of 3D technology to realize the drone body are just some of the scientific developments undertaken by the Russians in FPV UAS systems (X, 2023; Russians increase the range and stability of FPV drones, 2024).

Ukraine has also attached great importance to this segment. The accessibility of FPV drones has facilitated their wider operational use in the Russian-Ukrainian conflict. For Ukraine, the accessibility of FPV drones has made it easier to remain competitive even in the face of the numerical superiority of the Russians, against the background of the inconsistent supply of military equipment by the Western allies.

It is noteworthy that the development of this industrial sector in Ukraine has been accelerated, with a significant increase in the number of companies producing drones. Specifically, the number increased from seven in 2022 to about 80 by the end of last year (How Ukraine's cheap FPV drones are used on the Ukrainian battlefield, 2023). The considerable growth within the drone industry demonstrates how important these devices have become in the conflict. Due to their characteristics and ability to provide real-time imagery and intelligence, as well as the possibility of being equipped with munitions, FPV drones have become an integral part of surveillance and target engagement efforts. Moreover, increased affordability and reduced production costs have allowed Ukraine to develop its own FPV drone industry, which has increased the country's capabilities and resources in the face of complex conflict challenges, and has been able to operationally replace and complement much more expensive surveillance and weapon systems.

It is estimated that, by the end of 2023, about 50,000 drones of different types were being manufactured in Ukraine every month, the majority of which are FPV drones (Balashova, 2023). Moreover, the Ukrainian government has allocated about $1 billion this year for investment in its own manufacturing industry (Governmental Portal of Ukraine, 2023), one of the results being the KH-S7 drone in *figure 3*. This FPV-type drone can carry a weight of 1 kilogram within a range of up to 9.5 kilometres. It is also the Ukrainian government's intention to produce 1 million FPV drones by 2024 (Zafra, 2024), with 200,000 already produced in the first two months. (Since the beginning of 2024, Ukraine has produced about 200 thousand FPV drones, 2024).



Figure 3: Ukrainian KH-S7 FPV drone (Ukraine develops KH-S7 FPV drone, 2023)

On 1 July 2022, the Ukrainian government through the Ministries of Defence and Digital Transformation initiated the project *"The Army of Drones"*, which aimed to modernize and expand the use of drones in the Ukrainian military. The roles of this program were to facilitate the acquisition of drones, raise private funds for this purpose, carry out their maintenance and modernization, and train the personnel involved in their operation. The program has been a success, transforming the Ukrainian army into one modern and well-prepared for the challenges of the ongoing conflict (United 24, 2024; Army of Drones, 2024).

In addition, key players in the international community are supporting Ukraine's war effort. One example is the formation of the 11-member *"Drone Coalition"*, including the United Kingdom, Germany, and Poland, which recognizes the importance of drones in today's conflicts and the need to support Ukraine with drones. As a result, the coalition aims to support Ukraine's war effort with 1 million FPV drones (Joint Statement by the Drone Coalition's Ministers of Defence, 2024).

In a move designed to revolutionize the way contemporary military operations are carried out, Ukraine has set up a separate category of forces for Unmanned Systems Forces (USF), announced by President Zelensky in February and made a reality in June this year. Remarkably, it is the first nation to do so (Ukraine's Zelenskiy orders creation of separate military force for drones, 2024; Dangwal, 2024; Bielieskov, 2024). The main roles of the USF include coordination of combat units specialized on UAS, planning deep operations for these systems, identifying lessons and implementing them among the army force structures, developing and updating doctrine specific to the operation of unmanned aerial systems, or recruiting

and training personnel required for the operation of UAS (Hardie, 2024).This decision is a guarantor of increased efficiency in the use of FPV UAS systems in the context of the conflict in Ukraine.

Due to the importance of UAS systems, Ukraine has changed the organizational status of most of its brigades, each of which now includes a UAS company designed to engage targets, with one platoon operating FPV drones (Sahuquillo, 2024; Ukraine is betting on drones to strike deep into Russia, 2024).

Ukraine is also investing in drone research and development. For example, it intends to develop FPV-type drones based on artificial intelligence, which will provide the ability to counter enemy jamming signals and also to attack in swarms of interconnected drones that act compatibly and exchange information with each other in real time to complete the assigned mission (Hunder, 2024). Up to this point, research efforts are focused on elements that can be achieved more quickly, such as reducing engine noise levels or reducing the electromagnetic footprint (Hudson, 2023). These actions have attracted the attention of various international actors, who have begun to attach increasing importance to FPV UAS systems.

In an effort to adapt, the **US Army** is planning to field small commercial drones at the brigade level, based on lessons learned from the Russian-Ukrainian conflict. The process is well underway, with companies already selected for delivery (Judson, 2024). To test their effectiveness, some units have been equipped with such drones since late 2022 (Helfrich, 2022). In March, the US Army announced that it would equip other infantry units with small drones as part of the experiment (Chávez, 2024). According to US officials, infantry platoons of manoeuvre brigades will most likely be equipped with FPV drones starting in fiscal year 2026 (Skove, 2024).

The US Army's Manoeuvring Centre of Excellence is already organizing courses for small drone operators (US Army hosts inaugural drone competition at Fort Moore, 2024), as shown in *figure 4*. The establishment of a school specifically for training FPV drone pilots is also being considered, with the course to last 3-4 weeks (Skove, 2024).

Australia also recognizes the importance of FPV drones in contemporary conflicts. Thus, the Australian defence establishment recognizes the urgent need for the military to learn lessons from Ukraine. The creation of its own FPV drone capability, as well as a specialized training centre, is one of the future directions to follow in the effort to adapt the force structure to the challenges of the current operating environment.

China's military is already training with FPV drones (Kesteloo, 2024; Satam, 2024), and **Israel** is employing them in the conflict in the Gaza Strip (Antebi, 2024).



Figure 4: *Drone operators' course* (Borsari, 2023, p. 5)

Other major states such as **India** recognize the need to adapt their own armed structure by integrating FPV drones (The First Person View (FPV) Drone Revolution: India's Need to Adapt, 2024). In addition, the **Czech Republic** has decided to equip its own forces with FPV UAS systems under the new Army Reconstruction Concept of February this year (Domingo, 2024).

CONCLUSIONS

The way of conducting military operations specific to Western armies, known as manoeuvre warfare, is based exclusively on air-superiority. However, as the conflict in Ukraine has shown, where Russia has a clear superiority in terms of number of capabilities over Ukraine, it has not materialized. Thus, this premise of planning operations in an increasingly congested air environment may not be feasible. The widespread use of unmanned aerial systems has completely changed the way militaries operate. The ability to employ these aircraft can provide a significant operational advantage to any military structure. Moreover, the same contested operational environment poses increasing challenges to the use of medium and large drones (Borsari, 2023, p. 4). For this reason, small commercial drones, especially FPV drones, have become increasingly important in operations. Their low price, but also their high efficiency, have attracted increased attention from military structures.

Moreover, it is expected that advances in emerging technologies such as artificial intelligence will ensure an even greater impact of these systems on the battlefield by increasing their accuracy, operational efficiency and versatility (Ib.).

Within this framework, the present article aims to argue for the need to integrate these systems into the Romanian Army's force structures and operations.

It is recognised that the adaptation process is crucial for the ability of the armed forces to face new threats and challenges specific to the current and future operational environment. In this respect, operational lessons learned from the conflict in Ukraine can provide guidance and inspiration for future strategies, for the effective employment of the Romanian Armed Forces. One of these lessons is the integration of FPV drones into land operations as a multiplier of their effects.

The conflict in Ukraine has demonstrated that UAS systems, with varying degrees of sophistication, autonomy and functionality, have become an integral part of modern warfare. Successfully integrated into advanced combat tactics and operational concepts, drones can offer significant advantages to modern militaries by providing an effective capability for ISR, BDA or even fire support missions. In addition, their impact on the battlefield is amplified by rapid technological development, allowing for continuous improvements in performance and efficiency. Analysing operational lessons learned from the conflict in Ukraine can provide valuable insights into how military operations can be conducted in a complex and volatile environment.

The operational benefits, as well as the actions taken by various international actors regarding the acquisition of FPV drones, are just two solid arguments for the need to adapt the Romanian Army's force structures to the challenges of the current operational environment. In addition, there are some other factors that should be analysed and that may determine such a desire. The ageing population is one of them. It must be recognised that in the near future the human resources available for military service in the event of conflict will diminish. For this reason, we believe that the automation of the army must be a priority. We must also consider the moral impact of losing a drone in combat, which is insignificant compared to the loss of human life. Therefore, maintaining a high level of operational capability may be a consequence of equipping FPV drones. Cost versus effectiveness is also an important factor. The numerous situations in Ukraine show how important they can be in military operations. In addition, maintaining such equipment is certainly much cheaper than maintaining human personnel.

In order to integrate FPV UAS systems, the Romanian Army will have to consider more than just the acquisition of the aircraft. The selection and training of operators, the development of specific operational doctrines and the updating of existing ones, or the rethinking of the combat organisation of units are just some of the measures that will have to be taken. Therefore, we will conclude with what the former head of the Ukrainian Army, General Valerii Zaluzhnyi, wrote earlier this year in his famous article *On the modern design of military operations in the Russo-Ukrainian War: In*

the fight for the initiative: *"Perhaps the most important way to gain an advantage in today's conflicts is to master the entire arsenal of relatively cheap, modern and highly effective means that are rapidly developing"* (Zaluzhnyi, 2024), as is the case with FPV-type UAS systems.

BIBLIOGRAPHY:

1. *'$500 – Ukrainian drone, $3 million – Russia's most advanced tank, a skilled operator's hands – priceless'* (2 September 2024), https://english.nv.ua/nation/two ukrainian-fpv-kamikaze-drones-destroy-advanced-russian-t-90-proryv-tank-video-50350852.html, retrieved on 21 October 2024.
2. *3,500 Drone Operators Trained in Russia, Ministry of Defence Claims* (6 January 2024), Defense Express: https://en.defence-ua.com/news/3500_drone_operators_trained_in_russia_ministry_of_defense_claims-9104.html, retrieved on 16 July 2024.
3. *A Drone Worth a Few Hundreds of Dollars Against a 240-mm Mortar: Spectacular Destruction of the Tyulpan Mortar at a Distance of 10 km* (7 May 2023), https://en.defence-ua.com/news/a_drone_worth_a_few_hundreds_of_dollars_against_a_240_mm_mortar_spectacular_destruction_of_the_tyulpan_mortar_at_a_distance_of_10_km-6630.html, retrieved on 17 September 2024.
4. AAP-06 (2021). *AAP-06, NATO Glossary of terms and definitions (English and French).* NATO Standardization Office.
5. Antebi, L., Adar, O. (8 February 2024). *FPV Drones: From the Ukrainian Battlefield to the Middle East*, https://www.inss.org.il/publication/fpv/, retrieved on 22 July 2024.
6. Anwar, N. (7 February 2023). *World's largest drone maker is unfazed – even if it's blacklisted by the U.S.* CNBC, https://www.cnbc.com/2023/02/08/worlds-largest-drone-maker-dji-is-unfazed-by-challenges-like-us-blacklist.html, retrieved on 17 July 2024.
7. *Army of Drones* (2024), https://www.ukrainianworldcongress.org/united24/, retrieved on 11 July 2024.
8. Balashova, L., Melnyk, T. (23 November 2023). *Hands for wings. Ukrainian companies produce about 50,000 FPV drones every month*. Forbes, https://forbes.ua/innovations/ukrainski-inzheneri-pratsyuyut-u-boeing-ta-airbus-virobniki-droniv-strazhdayut-cherez-defitsit-kadriv-yak-rozvyazati-tsyu-problemu-20112023-17379, retrieved on 22 July 2024.
9. Barbu, F.-M., gl.-mr. (2024). *Războiul dronelor*. In *Gândirea militară românească*, no. 2, pp. 6-13.
10. Ben, B. (24 March 2024). *FPV drone tactics reshape conventional trench warfare in Russo-Ukrainian War*, Euromaidan Press, https://euromaidanpress.com/2024/03/22/both-ukraine-and-russia-rapidly-increase-the-use-of-fpv-drones-challenging-conventional-trench-fortifications/, retrieved on 22 July 2024.
11. Bielieskov, M. (20 February 2024). *Outgunned Ukraine bets on drones as Russian invasion enters third year*, Atlantic Council, https://www.atlanticcouncil.org/blogs/ukrainealert/outgunned-ukraine-bets-on-drones-as-russian-invasion-enters-third-year/, retrieved on 22 July 2024.

12. Borsari, F., Davis, Jr., G.B. “Skip” (2023). *An Urgent Matter of Drones*. The Center for European Policy Analysis’s (CEPA).
13. *Chuck Pfarrer Indications & Warnings* (26 December 2023), X, https://twitter.com/ChuckPfarrer/status/1739705046177042868, retrieved on 12 July 2024.
14. Collins, M.G. (2023). *Mobilizing the British Army*. In *The British Army Review* (182), pp. 6-9.
15. Dangwal, A. (16 June 2024). *Ukraine Launches World’s 1st Unmanned Systems Forces; Masters Robotic War Across Land, Sea & Air*, The Euroasian Times, https://www.eurasiantimes.com/ukraine-launches-worlds-1st-unmanned-systems-forces-masters-robotic-war-across-land-sea-air/, retrieved on 22 July 2024.
16. *DEX online* (2024), https://dexonline.ro/definitie/termit/definitii, retrieved on 11 July 2024.
17. Domingo, J. (22 May 2024). *Czech Republic Eyes Equipping Army with FPV Drones,* in The Defense Post, https://thedefensepost.com/2024/05/22/czech-republic-fpv-drones-army/, retrieved on 23 July 2024.
18. Edmonds, J.A., Bendett, S. (2023). *Russia’s Use of Uncrewed Systems in Ukraine.* Washington: The Center for Naval Analyses.
19. *FM 1-02.1 Operational Terms.* (2024). Washington DC: US Department of the Army.
20. *FPV Drone Control: Exploring Effectiveness and Risks in Military Operations in Ukraine* (7 May 2023), Defense Express, https://en.defence-ua.com/weapon_and_tech/fpv_drone_controle_exploring_effectiveness_and_risks_in_military_operations-6604.html, retrieved on 22 June 2024.
21. Gosselin-Malo, E. (19 July 2024). *Drone warfare in Ukraine prompts fresh thinking in helicopter tactics*, Defense news, https://www.defensenews.com/global/europe/2024/07/19/drone-warfare-in-ukraine-prompts-fresh-thinking-in-helicopter-tactics/, retrieved on 21 July 2024.
22. Governmental Portal of Ukraine (26 July 2023), https://www.kmu.gov.ua/en/news/denys-shmyhal-tsoho-roku-uriad-vydilyv-40-mlrd-hrn-dlia-investytsii-v-ukrainskykh-vyrobnykiv-bezpilotnykiv, retrieved on 2 August 2024.
23. Hambling, D. (10 November 2020). *The ‘Magic Bullet’ Drones Behind Azerbaijan’s Victory Over Armenia*, Forbes, https://www.forbes.com/sites/davidhambling/2020/11/10/the-magic-bullet-drones-behind--azerbaijans-victory-over-armenia/, retrieved on 22 July 2024.
24. Hardie, J. (21 June 2024). *Ukraine’s new Unmanned Systems Forces takes shape*, Long War Journal, https://www.longwarjournal.org/archives/2024/06/ukraines-new-unmanned-systems-forces-takes-shape.php, retrieved on 22 July 2024.
25. Helfrich, E. (7 December 2022). *Army Fields Its New RQ-28A Quadcopter Recon Drone,* The Warzone, https://www.twz.com/army-fields-its-first-u-s-designed-quadcopter-reconnaissance-drone, retrieved on 22 July 2024.
26. Horton, A., Korolchuk, S. (4 October 2023). *In Ukraine, explosive DIY drones give an intimate view of killing*. In The Washington Post, https://www.washingtonpost.com/world/2023/10/04/fpv-drone-ukraine-russia/, retrieved on 11 August 2024.
27. *How could FPV drones change warfare?* (4 April 2023), The Economist, https://www.economist.com/the-economist-explains/2023/08/04/how-could-fpv-drones-change-warfare, retrieved on 22 July 2024.

28. *How Realistic Are Russia’s Statements About Production of 4000 FPV-Drones Per Day?* (31 July 2024), Defense Express, https://en.defence-ua.com/news/how_realistic_are_russias_statements_about_production_of_4000_fpv_drones_per_day-11353.html, retrieved on 2 August 2024.
29. *How Ukraine’s cheap FPV drones are used on the Ukrainian battlefield* (9 October 2023), Army Recognition, https://armyrecognition.com/focus-analysis-conflicts/army/conflicts-in-the-world/russia-ukraine-war-2022/how-ukraine-s-cheap-fpv-drones-are-used-on-the-ukrainian-battlefield?highlight=WyJydXNzaWEiXQ%3D%3D#google_vignette, retrieved on 22 August 2024.
30. Hudson, J., Khudov K. (26 July 2023). *The war in Ukraine is spurring a revolution in drone warfare using AI,* The Washington Post, https://www.washingtonpost.com/world/2023/07/26/drones-ai-ukraine-war-innovation/, retrieved on 22 July 2024.
31. Hunder, M. (18 July 2024). *Ukraine rushes to create AI-enabled war drones*, Reuters, https://www.reuters.com/technology/artificial-intelligence/ukraine-rushes-create-ai-enabled-war-drones-2024-07-18/, retrieved on 22 July 2024.
32. *Joint Doctrine Publication 0-01.1 UK Terminology Supplement to NATO Term* (ed. B). (2023). UK Minister of Defence.
33. *Joint Statement by the Drone Coalition’s Ministers of Defence* (11 July 2024), Australian Government Defence, https://www.minister.defence.gov.au/statements/2024-07-11/joint-statement-drone-coalitions-ministers-defence, retrieved on 22 July 2024.
34. Jones, S.G., Harrington, J., Reid, C.K., Strohmeyer, M. (2023). *Combined Arms Warfare and Unmanned Aircraft Systems. A new era of strategic competition.* Washington DC: Center for Strategic and International Studies.
35. Judson, J. (12 September 2024). *Army picks two companies to get small drones to brigade combat teams*, Defense News, https://www.defensenews.com/land/2024/09/12/army-picks-two-companies-to-get-small-drones-to-brigade-combat-teams/, retrieved on 22 July 2024.
36. Kerry, C., Swed, O. (15 August 2024). *Small Drones for Big Militaries: The Way Ahead*, Army War College, https://warroom.armywarcollege.edu/articles/small-drones/, retrieved on 11 July 2024.
37. Kesteloo, H. (28 April 2024). *Chinese Military Trains with FPV Drones, DJI Avata and Drone Countermeasures*, https://dronexl.co/2024/04/28/chinese-military-trains-with-fpv-drones-dji-avata/, retrieved on 22 July 2024.
38. McFadden, C. (24 August 2023). *Ukrainian military unveils its new ‘SkyKnight’ bomber drone*, Interesting Engineering, https://interestingengineering.com/innovation/ukraine-own-bomber-drone, retrieved on 2 July 2024.
39. Milasauskas, T., Jaškūnas, L. (20 June 2024). *FPV drones in Ukraine are changing modern warfare*, Atlantic Council, https://www.atlanticcouncil.org/blogs/ukrainealert/fpv-drones-in-ukraine-are-changing-modern-warfare/, retrieved on 22 July 2024.
40. *Operational Environment 2024-2034: Large-Scale Combat Operations.* (2024). US Training and Doctrine.
41. *Putin wants “mass production” of drones in Russia* (28 April 2024), Ukrainska Pravda, https://www.pravda.com.ua/eng/news/2023/04/28/7399771/, retrieved on 22 July 2024.

42. Rhodes, C. (2024). *Small Aircraft, Sizeable Threats: Preparing Army to counter Small Uncrewed Aerial Systems*. In *Australian Army Occasional Paper* (24).
43. *Russia's Boomerang Copter-Class Small FPV Drones* (24 March 2023), UAS Vision, https://www.uasvision.com/2023/03/24/russias-boomerang-copter-class-small-fpv-drones/, retrieved on 2 July 2024.
44. *Russia Produces a Series of Ground FPV 'Kamikaze' Drones* (13 June 2024), UAS Vision, https://www.uasvision.com/2024/06/13/russia-produces-a-series-of-ground-fpv-kamikaze-drones/, retrieved on 22 July 2024.
45. *Russians increase the range and stability of FPV drones* (9 January 2024), Militarnyi, https://mil.in.ua/en/news/russians-increase-the-range-and-stability-of-fpv-drones/, retrieved on 22 July 2024.
46. Sahuquillo, M. (8 January 2024). *Night mission with a Ukrainian brigade operating bomb-carrying drones on the Bakhmut front,* pe El Pais, https://english.elpais.com/international/2024-01-08/night-mission-with-a-ukrainian-brigade-operating-bomb-carrying-drones-on-the-bakhmut-front.html#, retrieved on 22 July 2024.
47. Satam, P. (19 March 2024). *As 'Drone Piloting' Becomes New Military Domain, Chinese PLA Soldiers Fly FVP UAVs Through Tricky Hurdles*, https://www.eurasiantimes.com/plas-fpv-attack-uavs-and-redefine-the-infantry-role/amp/, retrieved on 12 July 2024.
48. *Since the beginning of 2024, Ukraine has produced about 200 thousand FPV drones* (29 February 2024), Militarnyi, https://mil.in.ua/en/news/since-the-beginning-of-2024-ukraine-has-produced-about-200-thousand-fpv-drones/, retrieved on 12 July 2024.
49. Skove, S. (14 May 2024). *FPVs, tethered drones could become formal Army programs in 2025,* Defense One, https://www.defenseone.com/threats/2024/05/fpvs-tethered-drones-could-become-formal-army-programs-2025/396573/, retrieved on 22 July 2024.
50. *The First Person View (FPV) Drone Revolution: India's Need to Adapt* (16 March 2024), https://defence.in/threads/the-first-person-view-fpv-drone-revolution-indias-urgent-need-to-adapt.4555/, retrieved on 22 July 2024.
51. *Ukraine develops KH-S7 FPV drone* (8 September 2023), Ukraine Ministry of Defence, https://mil.in.ua/en/news/ukraine-develops-kh-s7-fpv-drone/, retrieved on 22 July 2024.
52. *Ukraine is betting on drones to strike deep into Russia* (20 March 2024), https://www.economist.com/europe/2023/03/20/ukraine-is-betting-on-drones-to-strike-deep-into-russia, retrieved on 17 July 2024.
53. *Ukraine's Zelenskiy orders creation of separate military force for drones*. (6 February 2024), Reuters, https://www.reuters.com/world/europe/ukraines-zelenskiy-orders-creation-separate-military-force-drones-2024-02-06/, retrieved on 12 July 2024.
54. *Ukrainian FPV Drone Rams Russian Mi-24 Helicopter* (7 august 2024), UAS Vision, https://www.uasvision.com/2024/08/09/ukrainian-fpv-drone-rams-russian-mi-24-helicopter/, retrieved on 12 July 2024.
55. *Ukrainian FPV kamikaze drones attack Russian military equipment* (13 July 2023), Military News UA – X, https://twitter.com/front_ukrainian/status/1679395403077148673, retrieved on 12 July 2024.

56. *Ukrainian Military Destroyed Russian Murom-P Surveillance System Once Again* (7 May 2023), Defense Express, https://en.defence-ua.com/weapon_and_tech/ukrainian_military_destroyed_russian_murom_p_surveillance_system_once_againe_video-6631.html, retrieved on 22 July 2024.
57. *Ukrainian MoD highlights 'drone-on-drone' engagements over the battlefront*. (3 June 2024), European Security&Defence, https://euro-sd.com/2024/06/major-news/38485/drone-on-drone-over-ukraine/, retrieved on 12 July 2024.
58. *Ukrainian new heavy FPV drones with enhanced warheads will be „nightmare" for Russians* (4 July 2024), Kanal 13 – Youtube, https://www.youtube.com/watch?v=dCGXb0GPJfE, retrieved on 22 July 2024.
59. *United 24* (2024), https://u24.gov.ua/dronation?fbclid=IwAR3Ic0yzUMDvm71ErjsHpKjMUNOhu4GpWhGjxu6fT2abSpvLb0bEt33OUNc, retrieved on 17 June 2024.
60. *U.S. Army hosts inaugural drone competition at Fort Moore* (8 May 2024), https://www.wrbl.com/news/beehive-classic-u-s-army-hosts-inaugural-drone-competition-at-fort-moore/, retrieved on 22 July 2024.
61. Zafra, M., Hunder, M., Rao, A., Kiyada, S. (26 March 2024). *How drone combat in Ukraine is changing warfare*, Reuters, https://www.reuters.com/graphics/UKRAINE-CRISIS/DRONES/dwpkeyjwkpm/, retrieved on 22 July 2024.
62. *What are 'dragon drones', Ukraine's latest weapon against Russia?* (9 September 2024), Al Jazeera, https://www.aljazeera.com/news/2024/9/9/what-are-dragon-drones-ukraines-latest-weapon-against-russia, retrieved on 22 July 2024.
63. *X* (123 April 2023), https://x.com/Geopolitics_Emp/status/1645912003389583361, retrieved on 12 July 2024.
64. Zaluzhnyi, G.V. (2 February 2024). *On The Modern Design of Military Operations in The Russo-Ukrainian War: In The Fight for The Initiative*, https://nvkarta.com/project/library/uploads/military/analytics/(en)_ZALUZHNYI_MODERN_DESIGN_OF_MILITARY_OPERATIONS_Feb_1st_2024.pdf, retrieved on 22 July 2024.
65. https://www.defensemirror.com/news/36386/Russia_Tests_FPV_Drone_Carrier_in_Ukraine (22 March 2024), https://www.defensemirror.com/news/36386/Russia_Tests_FPV_Drone_Carrier_in_Ukraine, retrieved on 22 July 2024.
66. https://dexonline.ro/definitie/termit/definitii (9 September 2024), Al Jazeera, https://www.aljazeera.com/news/2024/9/9/what-are-dragon-drones-ukraines-latest-weapon-against-russia, retrieved on 2 July 2024.

EMERGING TECHNOLOGIES AND CHALLENGES IN HYBRID UNMANNED AERIAL VEHICLE OPERATIONS IN THE METAVERSE ERA

Florina Ghindescu COSTAȘ, PhD Student
University of Petroşani
Professor Roland Iosif MORARU, PhD Habil., BEng
University of Petroşani
Assistant Professor Ioana-Raluca ADOCHIEI, PhD, BEng
"Ferdinand I" Military Technical Academy, Bucharest
DOI: 10.55535/RMT.2024.4.09

With the maturity of UAV technologies and the expansion of the Internet of Things (IoT), unmanned aerial vehicles (UAVs) have become an essential component in multiple industries, representing a crucial tool for addressing current and future challenges. Integrating emerging technologies and advanced training methodologies for unmanned aerial vehicle operators is essential to ensure the efficient and safe use of these technologies. This research investigates critical gaps in understanding the emerging risks associated with human-machine interaction, from the perspective of occupational safety and health (OSH). While automation contributes to simplifying processes, extended reality (XR) facilitates the development of interactive educational resources, and augmented artificial intelligence (AAI) amplifies human cognitive capabilities through the use of advanced artificial intelligence (AI) algorithms. In the context of the industrial metaverse, these technologies offer significant opportunities for optimizing operational efficiency, supporting the training of drone operators in successfully managing the complexities of modern airspace.

Keywords: UAV operator training; industrial metaverse (AI, AAI); emerging technological risks; occupational safety and health (OSH); UAV;

INTRODUCTION

There is growing recognition that the professional environment is evolving rapidly due to technological advances and globalization. According to a report by PriceWaterhouseCoopers (PwC), headquartered in London, UK, AI could contribute up to 15.7 trillion USD to global economic growth by 2030 (Rao, 2017, p. 3). While AI focuses on task automation, augmented intelligence aims to integrate into the human experience rather than fully replace it, being designed to enhance our cognitive abilities and help us achieve higher levels of performance (Kim, 2022, p. 1). At the same time, intelligent automation technologies offer increasing opportunities, including for human resource management, but also present feasible technological and ethical challenges (Christenko, 2022, p. 6).

The impact of these technologies is evident both at the individual level, through the transformation of roles and required skills, and at the organizational level, through the need to reconfigure work processes and cultivate an organizational culture that fosters *human-machine collaboration*. The effects of technological changes on occupational health and safety (OHS) opportunities and challenges have always accompanied technological evolution (Rosen, 2022, p. 1). In this context, a rapidly evolving sector with significant potential, including within the European Union, is unmanned aerial vehicles (UAVs). Currently, UAVs are referred to by various terms, such as drones, remotely piloted vehicles (RPVs), remotely piloted aircraft (RPA), unmanned aircraft systems (UAS), and remotely piloted aircraft systems (RPAS). These terms have emerged at different stages of technological development or in various application scenarios but do not create ambiguity in context (Fan, 2020, p. 199). UAVs represent a class of devices that include multi rotor drones, as well as single-rotor and fixed-wing devices, hybrid versions, and potentially alternative propulsion systems essentially, robots capable of flight. Although the number of commercial drones has grown significantly, military applications still dominate the market.

In terms of autonomy, research presents a taxonomy with six levels (Eibin, 2021, p. 1) or ten levels of autonomy for UAVs (Sequeira, 2023, p. 2). While this taxonomy primarily targets military contexts, it also applies to UAVs operating in other scenarios. UAVs have brought significant changes to how we work and interact

with the environment, opening new opportunities for innovation and economic growth while offering advantages over conventional technologies (Gaurav, 2018, p. 12).

The key sectors benefiting from UAV technology include military, civil, and commercial domains, such as agriculture, construction and infrastructure, logistics and transportation, healthcare, environmental monitoring, defence, mapping and surveying, and scientific research missions. The diversity of UAS applications requires a tailored approach to operator training. Given that each industry and organization has specific requirements, a single certification may be insufficient. Therefore, more nuanced and use-case-specific training requirements are essential, as the lack of such training could lead to incidents (Williams, 2023, p. 1). The Federal Aviation Administration (FAA) highlights significant demand for UAV operators in the military and maritime sectors, providing valuable insights into the challenges faced by the US industry and emphasizing the need for clear standards for drone operation safety and operator training (Ib.).

Recent studies in AI and remotely piloted aircraft systems show that a fully autonomous system could significantly improve decision-making and the overall efficiency of missions (Eibin, ib.). These exponential advances are driven by both algorithmic innovations (sensorimotor learning in simulation) and system engineering improvements, covering the entire navigation flow: perception, planning, and control (Hanover, 2024, p. 17). Currently, drones that offer a balance between autonomy and human control remain relevant (Presamil, 2024, p. 1). Until fully autonomous systems can reliably manage the vast amount of data generated during flight in real time, human operators will remain essential to ensure the safety and performance of UAVs.

As AI becomes more robust, safety algorithms are becoming critical for UAV operations in complex and uncertain environments (Hanover, p. 18). Alongside technological progress, the global regulatory framework must be modernized to enable fully autonomous RPAS operations (Eibin, p. 2).

A recent study (Rahmani, 2023, p. 57) highlights that drone operators working in the gig economy have been overlooked in terms of occupational health and safety (OHS). The study explores human-UAV interaction, the dynamics of operator training through the adoption of new AI and XR technologies, and how OHS risks are affected by these changes. Digital technologies offer more efficient and flexible possibilities for military training, adapting to the complexity of modern operations (Jungck, 2023, p. 1). Recent findings show that human factors, rather

than technological defects, are the primary cause of most drone accidents, such as a lack of situational awareness and poor decision-making (Rahmani, pp. 63-64).

The human-machine interface is an emerging risk in occupational health and safety (OHS), but it also offers a pathway to improving safety, highlighting the importance of proper design as UAV autonomy levels increase (Sequeira, 2023, p. 7). In the era of the metaverse, digital technologies such as AI and XR have a significant impact on the training process, providing personalized learning experiences. While the integration of these technologies enhances operational efficiency, it also introduces new occupational health risks.

This new paradigm requires a holistic approach that considers both the technological complexity and the impact on the occupational health of UAV operators, within a dynamic and ever-changing regulatory framework. The lack of empirical data on associated risks complicates the development of effective risk mitigation strategies. Identifying research gaps is essential for developing informed policies that ensure operator safety and address unaddressed risks.

This study employs the PRISMA methodology for the selection and critical analysis of relevant literature from academic and industrial sources. The sources presented below have been filtered based on the irrelevance to the following areas: unmanned aerial vehicles (UAVs), occupational health and safety (OHS), and the use of XR technologies in UAV operator training.

THEMATIC ANALYSIS

UAV Integration, Digital Surveillance, Ethics, and Space

Research conducted within European Commission projects – ranging from the improvement of flight standards (aw-drones.eu, 2021) and the coordination of UAV fleets and their integration into air traffic (labyrinth2020.eu) to the development of solutions for countering threats, including neutralizing UAVs operating in restricted areas (alladin2020.eu) and exploring the potential of 5G technology (5gdrones.eu) – has marked significant progress in drone integration. However, these initiatives have also identified potential safety threats posed by UAVs. It is not surprising that technological issues no longer dominate research concerns. Instead, organizational, managerial, and operational impacts on performance and safety are becoming the primary focus (Sequeira, p. 4).

Despite the clear benefits of UAV usage, their rapid proliferation in various work environments raises social and ethical dilemmas, particularly regarding privacy

invasion and public safety risks (Rahmani, p. 63). Initiatives led by organizations such as NATO, along with discussions at international forums, play a critical role in shaping a collective response to these emerging challenges. These initiatives emphasize the importance of collaboration in securing airspace, especially within the context of contemporary digital conflicts. The significance of cooperation is further highlighted by ongoing efforts to develop a comprehensive legal and ethical framework for digital space operations, ensuring a balanced approach that accounts for both military and civilian interests (Botezatu, 2024, p. 6).

Another important aspect is the growing role of artificial intelligence (AI) and augmented artificial intelligence (AAI) in UAV surveillance and control. These technologies facilitate efficient risk management and enhance operational efficiency. AI enables the automation of complex processes, while AAI improves human capabilities by integrating automated analysis with human decision-making, offering safe and effective solutions for UAV operations in both civilian and military contexts.

Emerging technologies such as 5G networks and the Internet of Things (IoT) also play a crucial role in managing air traffic and communication networks. However, these advancements bring additional risks, including cybersecurity vulnerabilities, which require appropriate security measures and standardization efforts.

To ensure the safe and efficient integration of UAVs into airspace, an integrated regulatory framework is essential – one that balances both military and civilian interests. Strict regulations supported by a solid ethical framework will prevent the misuse of surveillance technologies and contribute to public safety and privacy protection.

Drones have significantly transformed the strategic conduct of warfare, offering substantial advantages in power projection, operational efficiency, reduction of political and humanitarian risks, and adaptability to asymmetric and cyberwarfare (Barbu, 2024, pp. 11–13). The use of unmanned aerial vehicles (UAVs) in military missions not only reduces the risk of human casualties, thereby enhancing operational safety in conflict zones, but also generates significant cost savings compared to manned aircraft operations (Fan, 2020, p. 204). Additionally, UAVs can access confined or inaccessible spaces, as well as flammable or toxic environments, making them essential for high-risk operations (Rahmani, p. 53).

The National Institute for Occupational Safety and Health (NIOSH), in an integrated approach to workplace safety, classifies UAVs *as "professional service robots"*, highlighting their role in performing dangerous or repetitive tasks, thereby

reducing the risk of accidents and incidents at work (NIOSH, 2024, p. 1). Consequently, the application of UAV systems in the military domain has become increasingly common and will continue to shape new military capabilities. Since the emergence of the first UAV in the United Kingdom in 1917, drone technology has evolved from target drones and reconnaissance aircraft to sophisticated, multifunctional systems capable of executing a wide range of complex military operations (Fan, p. 204).

Since the early 1990s, next-generation UAVs have been widely deployed in conflicts and wars, performing various missions, including reconnaissance, firepower engagement, electronic countermeasures, communication support, and logistics transport. The *"unmanned"* characteristic of these systems is gradually becoming a core component in the development of modern weaponry and their practical use on the battlefield (Ib.).

To ensure that military forces possess the capabilities necessary to successfully complete missions and address future challenges, decades of military research have focused on improving team and equipment efficiency. The military, alongside the aviation community, has been a leader in advancing research on team dynamics and performance, shaping the development of *"team science"* (Goodwin, 2018, p. 331).

Defining events, such as the 2001 terrorist attacks, catalysed the development of combat capabilities for unconventional, dynamic, and unpredictable environments. These efforts have ranged from developing specific tools for assembling military support teams to substantial investments in team training technologies (Ib., p. 328). Technological advancements have created new arenas for military competition, such as cyberspace, fostered a reliance on information superiority as a strategic advantage, and introduced robots and AI-based software systems into decision-making and combat environments.

A relevant example is the TADMUS (Tactical Decision Making Under Stress) program, which systematically explored the dynamics of decision-making teams under stress, driving research in both military and non-military domains (Ib.). Today, the use of drones in military conflicts, such as the war in Ukraine, has redefined warfare tactics, offering critical advantages in surveillance, precision strikes, rapid response, and integration into complex information networks, while also reducing the risks and costs associated with traditional military operations (Barbu, 2024, p. 10).

While the commercial sector explores the concept of the metaverse, synthetic environments used by military forces worldwide allow for complex military training

in a controlled setting. These environments, integrated with technologies such as artificial intelligence (AI), augmented reality (AR), and simulation, provide realistic and effective training for armed forces. Additionally, secure cloud infrastructure ensures the protection of sensitive data and information, which is essential in the context of military training (Jungck, 2023, p. 1).

At the national level, research programs aim to develop and implement new standards for interoperability and cybersecurity. In this regard, the lack of technological know-how among developers can have serious implications for the cybersecurity of these systems (Vevera, 2018, p. 72). In the case of UAVs, addressing cyber risks has led to digital solutions such as platforms that ensure the transmission of critical data through public telecommunications networks, the cloud storage of sensitive information, and segregated data access using immutable Blockchain technologies and military-grade encryption (DIGITALI, 2023, p. 1).

In conclusion, the use of UAVs in military operations is becoming increasingly flexible and dynamic, supported by multidimensional platforms that operate simultaneously across land, sea, air, and space. New tactics and combat methods are emerging, such as the coordinated operation of *"manned and unmanned aircraft"* and *"drone swarms"*, enhancing the combat capabilities of entire systems (Fan, 2020, p. 204). For instance, the HADRON project aims to facilitate UAV operations by ensuring scalability and incorporating artificial intelligence algorithms to reduce the workload on operators, allowing them to focus more on supervisory roles (Casado Fauli, 2024, p. 4).

However, military revolutions require more than just the widespread adoption of new technologies. Armed forces must develop new operational concepts, integrate technological capabilities into complex military systems, and adapt their organizational culture and structure to these developments. A true revolution in military affairs involves not only technological innovations but also a doctrinal component tailored to the new realities of the battlefield (Barbu, 2024, p. 10).

The Metaverse in Industry 5.0: A Human-Centred Approach

The metaverse is currently regarded as an inevitable trend in the process of social informatization and virtualization, representing the final stage of the Internet's development. Concepts such as virtual reality (VR), augmented reality (AR), mixed reality (MR), and extended reality (XR) together shape the framework for the new era of interactions between the digital and real worlds (Tang, 2024, p. 2). The *"Fourth Industrial Revolution"*, which began in 2012, and its transition to Industry 5.0, is characterized by the digital transformation of organizations, driven by machine-to-machine collaboration, connectivity, and digital enablers such

as the Internet of Things (IoT), Big Data, intelligent systems, cloud computing, virtualization, collaborative robotics, and artificial intelligence (Moraru, 2024, p. 192).

However, this transition also brings emerging risks, creating opportunities for proactive research in security science. By merging the real and virtual realms, the metaverse offers enormous potential to revolutionize not only the industrial sector but also services, enabling personalized experiences and improving operational efficiency. The seamless synergy between Industry 5.0's human-centred principles and the metaverse's ability to deliver personalized value establishes a solid foundation for future technological development (Mourtzis, 2023, p. 1110).

The COVID-19 pandemic accelerated the shift of life and work towards digital spaces, reinforcing the metaverse's role in reshaping professional and social interactions. These virtual worlds allow users – represented by avatars – to interact with each other, create, and consume content in immersive, scalable, synchronized, and persistent environments (Weinberger, 2022, p. 1). The integration of emerging technologies, such as brain-computer interfaces (BCIs), into the metaverse promises to seamlessly fuse virtual experiences with human cognitive capabilities, enabling far more complex and personalized interactions (Mourtzis, p. 1107).

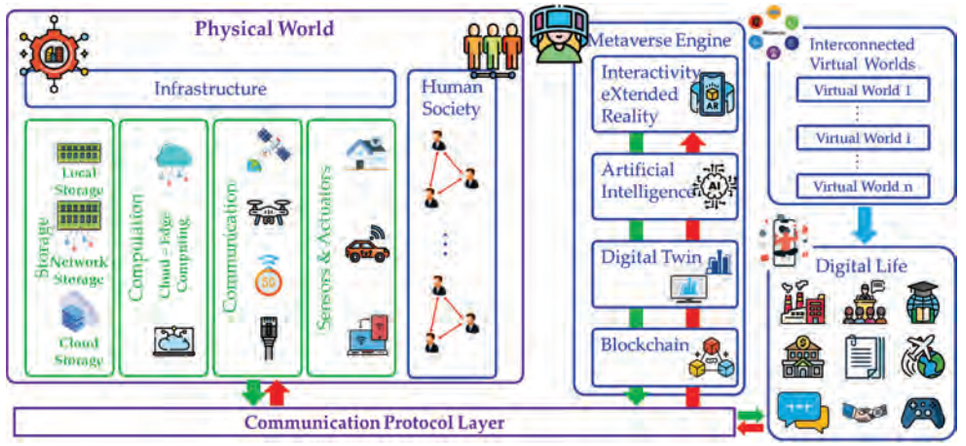


Figure 1: Technical architecture for the Industrial Metaverse
(Mourtzis, 2023)

The convergence of the metaverse with advanced brain-computer interfaces (BCIs) promises to seamlessly merge virtual experiences with users' cognitive abilities. By detecting and translating brain activity into computer-readable commands, brain-computer interfaces have the potential to radically transform how people interact with technology. Although still in its early stages of development, this technology shows promise, offering unlimited opportunities for application in various fields, including healthcare and education (Ib.).

To ensure the sustainable development and widespread adoption of these technologies, the metaverse must consistently prioritize user experience, protect fundamental rights, and proactively address the ethical and security challenges associated with these virtual environments (Ib.). Such an approach will be essential in building a secure and inclusive digital ecosystem capable of improving human interactions and preventing potential risks related to data protection and privacy.

At the same time, the metaverse provides an ideal framework for researching and testing artificial intelligence (AI) algorithms applied to drones, thereby accelerating technological progress and its applicability in the real world. Recent projects, such as DARPA's Fast Lightweight Autonomy (FLA) and the European Research Council's Agile Flight, reflect the accelerated race to develop and integrate artificial intelligence into the construction of fully autonomous drones (Hanover, 2024, p. 17). Despite significant technological advancements, considerable challenges remain, including the gap between the performance of drones in controlled environments and their applications in the real world. Issues such as operational safety, task generalization, and adaptability to various flight environments require innovative solutions and in-depth research to enable a seamless transition of autonomous drones into commercial and military applications (Ib.).

While autonomous drones have demonstrated performance exceeding human capabilities in controlled conditions, developers face the need to find trade-offs between safety and performance, especially in the case of agile flight. In this context, accelerating the development of the production industry for advanced UAV systems will continue to facilitate innovation in emerging technological applications, such as aerospace manufacturing, the widespread use of artificial intelligence, communication networks, and advanced materials (Fan, p. 204).

As these technologies become increasingly integrated into Industry 5.0, they will not only transform manufacturing and logistics but will also open up new opportunities for innovation in the mid and high-value chain, thus facilitating a transition to intelligent, efficient, and human-centred production.

Disruptive Technologies and Emerging Trends in UAV Research

A recent analysis of UAV research trends from 2020 to 2023 has revealed a significant focus on developing sophisticated artificial intelligence (AI) tools capable of enhancing UAV performance in various domains, such as object detection, optimal trajectory planning, and autonomous mission execution. Emerging technologies identified include the Internet of Things (IoT, 4%), deep learning (DL, 8%), machine learning (ML, 4%), and reinforcement learning (RL, 3%), which open up new possibilities for the development of autonomous and intelligent

systems (Telli, 2023, p. 5). These trends indicate a significant transformative potential of UAV technologies, with applications in numerous fields, but also with significant challenges related to the complexity and security of these systems.

As UAVs become more robust and are used for an ever-wider range of purposes, the airspace is becoming increasingly congested. In this context, artificial intelligence plays a crucial role in integrating manned and unmanned aircraft, facilitating the safe sharing of airspace among users and the advanced implementation of U-space services, in accordance with European standards (EASA, 2024, p. 1). This integration is essential to ensure efficient air traffic management in an increasingly complex and competitive environment.

However, the implementation of new technologies is not without risks and challenges. Machine learning systems raise issues related to operational complexity and cybersecurity, and the ethical implications of using these technologies in military or civilian contexts require special attention. To guarantee the reliability and robustness of AI systems in these domains, a hybrid approach combining machine learning (ML, DL) models with logical and knowledge-based models is recommended. This type of hybrid AI would allow for the exploitation of both data and human expertise, ensuring a better understanding of system behaviour and increasing the level of confidence in the decisions made by these systems (EASA, 2023, pp. 6-19).

In this direction, explainable AI (XAI) has become a critical area of research, addressing the need for transparency and understanding in automated decision-making processes. AI systems that use deep learning (DL) methods rely on multi-layer neural networks to solve complex problems such as object classification or autonomous driving. The role of explainability is to provide clarity on how AI arrives at certain decisions, which improves the integration of these technologies into airborne combat systems, facilitating more informed tactical decisions and progress in combat strategy (Saldiran, 2024, p. 2).

The explainability of these systems is essential to build trust among pilots and UAV operators in the decisions made by autonomous or semi-autonomous drones. This trust is crucial for pilots to be able to focus on more complex tasks and make superior strategic decisions. Explainability allows users to build more detailed mental models of AI operation, thus improving human-AI collaboration and facilitating the use of autonomous drones in complex combat environments (Ib., p. 1).

In the long term, it is estimated that neural networks will replace every stage of the UAV navigation flow, similar to what has been observed in computer vision and natural language processing. This progress will require substantial innovations,

including efficient computing architectures, pre-training strategies, and rapid adaptation to unforeseen conditions (Hanover, 2024, p. 18). In this context, flight simulators have become an essential tool for training UAV pilots and testing autonomous drone control algorithms.

Today, photorealistic simulations, such as AirSim, FlightGoggles, and Flightmare, represent advanced technologies that have accelerated research in the field of autonomous flight and allow for the testing of complex scenarios in a safe and controlled environment (Ib., p. 13). AI-based simulations use techniques such as deep learning (DL) and reinforcement learning (RL), which allow them to accurately model drone behaviour in unforeseen and diverse situations. These technologies play a central role in the development of fully autonomous drones, being essential for optimizing their performance and safety (Amarasooriya, 2024, p. 127).

In an effort to improve control interfaces for UAVs, innovative technologies such as touchscreens, gesture-based control, voice recognition, and augmented reality (AR) have been explored. These solutions contribute to improving user interaction with the drone and increasing situational awareness, thus increasing operational efficiency (Casado Fauli, p. 4).

At the same time, the exponential evolution of the field of artificial intelligence has led to the development of advanced research programs that investigate the applicability of computer vision in controlling autonomous drones. For example, brain-computer interface (BCI) technologies are testing alternative ways of controlling drones, allowing operators to control UAVs through commands generated directly from brain activity. Recent tests have demonstrated an accuracy of 95.5% in controlling a quadcopter, but this technology has not yet been widely adopted (Dumitrescu, 202, p. 1).

Multidisciplinary technologies will continue to be integrated into UAV applications, and disruptive innovations will generate new solutions for current and future challenges. Ultimately, it is essential to establish clear rules for UAV operation, including for swarms of autonomous drones, to ensure operational safety and security (Telli, p. 33). These aspects are fundamental for the safe and responsible use of autonomous drones, as well as for protecting users and airspace.

Unmanned Aerial Vehicles (UAVs): Occupational Safety and Health Implications, Emerging Risks and Research Gaps

The continuous introduction of new technologies and work tools generates new risks for the health and safety of workers. Therefore, OSH risk assessment must be a dynamic and adaptive process, in accordance with legislative regulations (EU-OSHA, 2021, p. 1). EU-OSHA's prospective studies play a crucial role in anticipating

these risks and promoting a culture of prevention. Thus, the specific training programs will address the achievement of the different required qualification levels of the drone pilots depending on the type of drone, the autonomy level of the drones, varied and optimized for the use case of the drone (Casado Fauli, p. 1).

Research priorities are dynamic. Privacy, security and acceptance were the main concerns, although their dominance is declining. Also, understanding the social impact of drones, particularly in terms of human interactions and regulatory issues, is a key problem. Research gaps reported in the UAV literature are mainly related to organizational/management aspects and are closely related to risk minimization (Sequeira, pp. 11-13).

Figure 2 summarizes the main research as arising from the currently envisaged applications for UAVs and the associated concerns.

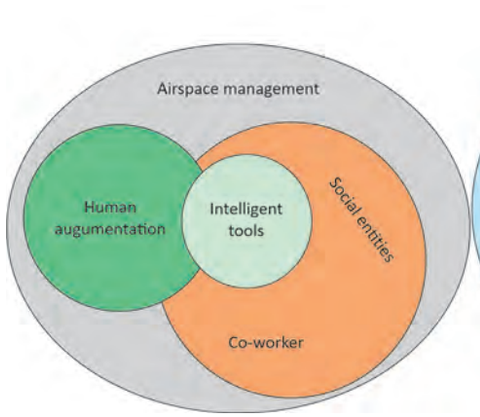


Figure 2: Research gaps in the field of UAVs

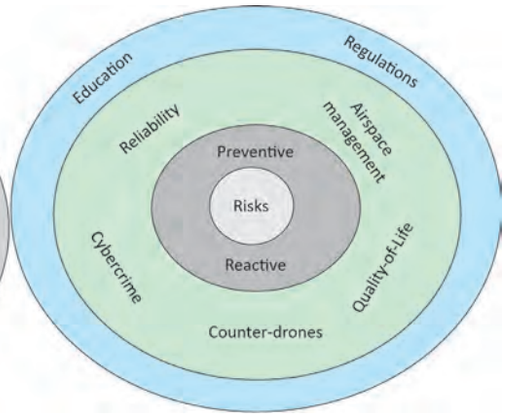


Figure 3: UAVs-associated risk management

(Sequeira, 2023)

Risks in the UAV field are commonly identified as: drone pilot/audience injury (physical to psychological); breach of confidentiality; generating liability, creating general property damage, including the UAV itself. These risks are not independent and their management must take into account several factors (Sequeira, pp. 11-13).

Since the metaverse is generally described as a space constituted by XR (VR, XR) technologies, the worker safety and health risks identified within XR also apply to those associated with the metaverse. Thus, the need to learn new skills and interact with new equipment, to reduce physical interactions, as well as the isolation and risks of interacting with and between avatars, have the potential to cause stress and are identified as psychosocial risks (Grassini, 2024, p. 1). Potential pathogen contamination of the equipment worn by the VR user (HMDs) is identified

with biological hazards. Ethical-legal risks refer to the new and unregulated nature of technology, the ethical implications of digital interactions, and the technical characteristics of technology that make them prone to privacy violations (EU OSHA, 2024, pp. 1-3,7-8).

FUTURE RESEARCH DIRECTIONS

The new paradigm of training unmanned aerial vehicle (UAV) pilots is not merely an extension of existing aviation practices but defines a distinct discipline that requires a detailed understanding of technological complexities, regulatory frameworks, and the impact of the training process on occupational health. Advanced simulators (Amarasooriya, p. 127), combined with synthetic environments and augmented reality, offer training solutions with unprecedented levels of immersion and interactivity, preparing operators for the challenges of future airspace and ensuring operational excellence (Wiegand, 2023, p. 1).

Although UAV pilots frequently adopt safety practices, the hazards associated with using unmanned aerial vehicles during training and operations remain insufficiently documented in the literature, necessitating further research (Rahmani, 2023, pp. 63-64). In this context, a dynamic review of safety standards and procedures is needed to keep pace with new technological and operational challenges.

The current study does not aim to provide an exhaustive action plan but highlights the need for an approach based on concrete data and the reform of occupational safety and health policies. The use of the PRISMA methodology to filter the available literature clearly demonstrates the need for proactive risk management associated with these evolving technologies.

Future research directions should focus on evaluating the current tools used to analyse the effects of virtual environments on UAV pilots, investigating best practices in recruitment and training, and examining the ethical challenges associated with the use of human-UAV interfaces and intelligent technologies.

The technological challenges posed by new interfaces and autonomous systems must also be explored to ensure the safe and efficient integration of UAVs into various fields of activity. Future research will need to address in particular the risks to occupational health and safety in this context of rapid development of disruptive technologies.

CONCLUSIONS

This paper identifies significant gaps in the existing literature, particularly regarding the occupational safety and health of unmanned aerial vehicle (UAV) pilots. The original contribution consists of a critical synthesis of the existing literature, identifying weaknesses and the need to develop risk assessment tools integrated into UAV platforms, as well as educational models based on augmented (AR) and virtual reality (VR) simulations. These models can be used to train pilots in a safe and efficient manner.

The analysis highlights the lack of empirical studies on emerging risks associated with UAV operation and underlines the importance of integrating emerging technologies into the training process to mitigate these risks. This approach provides a solid foundation for formulating policies and recommendations aimed at improving occupational safety and contributing to the creation of a robust regulatory framework.

As aviation training technology evolves, the training of UAV pilots faces a unique set of challenges, particularly regarding regulatory aspects, technological advancements, and operational risk management. The rapid pace of innovation often outpaces the development of standardized training protocols. In addition, public perception of unmanned aerial vehicles use and the social responsibility of operators play a crucial role in establishing an ethical framework for these technologies.

Digital transformation should not be analysed solely in terms of increased productivity but also in terms of new professional roles and the need for continuous learning. Emerging technologies such as IoT, Big Data, cloud computing, unmanned aerial vehicles, and the metaverse redefine the interactivity between the human factor and technology in environments characterized by volatility, uncertainty, complexity, and ambiguity (VUCA). The incorporation of digitalization opens new opportunities for innovation and optimization, providing solutions for preventing occupational risks and improving safety and health in complex environments.

BIBLIOGRAPHY:

1. Achimowicz, J.Z. (2024). *Autonomic Drones with Quantum Computing Artificial Intelligence?* DOI: 10.13140/RG.2.2.12642.71364, retrieved on 22 August 2024.
2. Amarasooriya, S. (2024). *Mathematical and Machine Learning Based Methods for UAV Simulation: A Systematic Literature Review*, https://doi.org/10.5281/zenodo.1108448, retrieved on 5 August 2024.
3. Badea, L. (2023). *Tehnici avansate de Inteligență Artificială în știință și domenii aplicative*, https://ici.ro/ro/proiecte-in-derulare/program-nucleu-future-tech-2023-2026/, retrieved on 20 August 2024.

4. Barbu, F.M. (2024), https://gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20GMR/2024/2/BARBU.pdf, retrieved on 6 August 2024.
5. Botezatu, U.E. (2024). *Cyber Orbits: The Digital Revolution of Space* (Security National Security in the Digital and Information Age, Sally Burt editor, on-line), https://www.intechopen.com/online-first/1175598, p. 6, DOI: 10.5772/intechopen.1005235, retrieved on 1 October 2024.
6. Casado Fauli, A.M (2024). *HADRON: Human-friendly Control and Artificial Intelligence for Military Drone Operations*, https://arxiv.org/html/2408.07063v1, retrieved on 21 August 2024.
7. Christenko, A. (2022). European Agency for Health and Safety at Work. Artificial intelligence for worker management: risks and opportunities, https://osha.europa.eu/sites/default/files/documents/ai-worker-management_en.pdf, retrieved on 5 August 2024.
8. DIGITALI (2023), https://digitalio.ro/2023/10/30/oves-enterprise-lanseaza-o-platforma-de-secu-ritate-pentru-retele-de-drone-si-avioane-bazata-pe-blockchain-si-ai/, retrieved on 5 August 2024.
9. Dumitrescu, C. (2021). *Using Brain-Computer Interface to Control a Virtual Drone Using Non-Invasive Motor Imagery and Machine Learning*, retrieved on 21 August 2024.
10. EASA (2023). *Artificial Intelligence Roadmap 2.0 Human-centric approach to AI in aviation*, European Union Aviation Safety Agency, https://www.easa.europa.eu/en/document-library/general-publications/easa-artificial-intelligence-roadmap-0#:~:text=The%20EASA%20Artificial%20Intelligence%20Roadmap,deliverables%20and%20anticipated%20rulemaking%20activities, retrieved on 22 August 2024.
11. EASA (2024). Artificial Intelligence and Aviation, europa.eu, retrieved on 7 August 2024.
12. EU OSHA (2021-2027). *EU Strategic Framework on Health and Safety at Work*, https://osha.europa.eu/ro/safety-and-health-legislation/eu-strategic-framework-health-and-safety-work-2021-2027, retrieved on 21 August 2024.
13. Eibin, M. (2021). *Survey of RPAS Autonomous Control Systems Using Artificial Intelligence*, IEEE Access.
14. Fan, B. (March 2020). *Review on the Technological Development and Application of UAV Systems*. In *Chinese Journal of Electronics*, vol. 29, no. 2.
15. Gaurav, S. (2018). *Unmanned aerial vehicle classification, applications and challenges: A review*. Preprints v1, https://doi.org/10.20944/preprints201811.0601, retrieved on 22 August 2024.
16. Goodwin, G.F. (2018). *The Science of Teams in the Military: Contributions from over 60 Years of Research* (In the public domain), vol. 73, no. 4, pp. 322-333. American Psychological Association, http://dx.doi.org/10.1037/amp000025, retrieved on 5 August 2024.
17. Grassini, S. (2024). *Worker exposure to virtual and augmented reality and metaverse technologies: how much do we know?*, EU OSHA, https://osha.europa.eu/sites/default/files/documents/worker-exposure-virtual-reality_discussion_paper_EN.pdf, retrieved on 4 August 2024.
18. Hanover, D. (2024). *Autonomous Drone Racing: A Survey*, IEEE, https://ardupilot.org/, https://px4.io/, retrieved on 22 July 2024.
19. Jungck, P. (2023), https://www.baesystems.com/en-us/feature/the-future-of-military-training-synthetic-environments-and-the-military-metaverse, retrieved on 11 August 2024.
20. Kim, J. (2022). *Bridging Human Intelligence and Artificial Intelligence. Augmented Intelligence: Enhancing Human Decision Making,* pp. 151-170. Springer.

21. Moraru, R.I. (2024). *Challenges and opportunities in occupational health and safety digitalization*, in *Digital Transformation*, Series: Intelligent Systems Reference Library, Booksubtitle: Technology, Tools, and Studies, pp. 189-213, editors Lucian-Ionel Cioca, Larisa Ivașcu, Florin Gheorghe Filip, Doina Banciu; SPRINGER Publishing House, eBook ISBN: 978-3-031-55952-5; ISSN: 1868-4394, Hardcover ISBN: 978-3-031-55951-8, https://doi.org/10.1007/978-3-031-55952-5, retrieved on 22 August 2024.
22. Mourtzis, D. (2023). *The Metaverse in Industry 5.0: A Human-Centric Approach towards Personalized Value Creation*, https://doi.org/10.3390/encyclopedia3030080, retrieved on 2 August 2024.
23. NIOSH (2024). *Robotics in the Workplace: An Overview*, https://www.cdc.gov/niosh/robotics/about/, retrieved on 22 August 2024.
24. Rahmani, H. (2023). *Working under the Shadow of Drones: Investigating Occupational Safety Hazards among Commercial Drone Pilots*, DOI:10.1080/24725838.2023.2251009, retrieved on 22 August 2024.
25. Rao, A.S. (2017). *Sizing the prize – What's the real value of AI for your business and how can you capitalise?*, https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf, retrieved on 5 August 2024.
26. Rosen, P.H. (2022). *Artificial intelligence, advanced robotics and the automation of tasks at work: taxonomy, policies and strategies in Europe*, https://osha.europa.eu/sites/default/files/AI-based-systems_EN.pdf, retrieved on 22 June 2024.
27. Saldiran, E. (2024). *Towards Global Explainability of Artificial Intelligence Agent Tactics in Close Air Combat*, https://doi.org/10.3390/aerospace11060415, retrieved on 22 August 2024.
28. Sequeira, J.S. (2023). *Unmanned aerial vehicles: implications for occupational safety and health*, https://osha.europa.eu/sites/default/files/Unnamed-aerial-vehicles-and-OSH_en.pdf, EU-OSHA, retrieved on 22 August 2024.
29. Tang, Y. (2024). *The application of metaverse in occupational health*, doi: 10.3389/fpubh.2024.1396878, retrieved on 5 August 2024.
30. Telli, K. (2023). *A Comprehensive Review of Recent Research Trends on Unmanned Aerial Vehicles (UAVs)*, https://doi.org/10.3390/systems11080400, retrieved on 22 August 2024.
31. Vevera, A.V. (2018). *Factorul uman vs. securitatea cibernetică/Human resource vs. cybersecurity*, doi: 10.13140/RG.2.2.28728.62722, retrieved on 22 August 2024.
32. Vevera, A.V. (2023). *Sisteme de comunicație reziliente și interoperabile bazate pe tehnologii distribuite și identitate digitală auto-suverană (RoDID)*, https://ici.ro/ro/proiecte-in-derulare/program-nucleu-future-tech-2023-2026/, retrieved on 5 August 2024.
33. Weinberger, M. (2022). *What is Metaverse? A Definition Based on Qualitative Meta-Synthesis*, https://doi.org/10.3390/fi14110310, retrieved on 22 August 2024.
34. Wiegand R. (2023), https://www.baesystems.com/en/project-odyssey-to-form-backbone-of-new-military-training-collaboration, retrieved on 27 August 2024. [
35. Williams, K.W. (2023). *Air Carrier Operations Survey: Training Requirements*, pp. 6. 24, 25; FFA, DOT/FAA/AM-23/09, Aviation Safety, Office of Aerospace Medicine, Washington, D.C. 20591, https://www.faa.gov/data_research/research/med_humanfacs/oamtechreports/media/UAS%20Air%20Carrier%20Operations%20Survey-Training%20Requirements_0_0.pdf, retrieved on 4 August 2024.

TABLE TOP ASSESSMENT GAMES
– A METHOD FOR ANALYSING FUTURE CAPABILITIES –

Lieutenant Colonel (N) Senior Instructor Alexandru-Lucian CUCINSCHI, PhD
"Carol I" National Defence University, Bucharest
DOI: 10.55535/RMT.2024.4.10

The article explores the role and application of table top assessment games in the process of developing and refining concepts and, consequently, capabilities, highlighting the benefits of conducting these activities in complex environments. Assessment games are structured sessions of discussions and role-playing used to simulate hypothetical scenarios, thereby enhancing decision-making capabilities and strategies through risk reduction, improved communication, and the promotion of creative problem-solving. In the military context, these exercises are essential for developing the capabilities required by new concepts, such as multi-domain operations. Their development requires not only the adaptation and implementation of new technologies but also complex coordination among various relevant actors, including the defence industry. The methodology detailed in the article analyses the differences and specific uses of some types of assessment games, such as the Concept Development Assessment Game/CDAG, highlighting the process of experimentation and concept evaluation. This exploration aims to emphasize the importance and applicability of these games in anticipating challenges and generating efficient solutions that contribute to better organizational preparedness and resilience.

Keywords: strategy; military capabilities; table top assessment game; technology; scenario;

INTRODUCTION

Table top assessment games (TTAG), also known as table top exercises (TTX), are an innovative and practical approach used in various fields to simulate real-world scenarios and evaluate strategies and decision-making processes. These exercises are frequently used in the Armed Forces, emergency management, corporate strategy development, and even education, serving as a versatile tool for training and analysis.

Table top assessment games are structured, discussion-based sessions, designed to assess and improve the effectiveness of strategies and responses in hypothetical situations. Participants engage in role-playing, making decisions based on the scenario presented and discussing the potential outcomes and consequences of their actions. These exercises are especially useful in complex environments where understanding the interaction of multiple factors is crucial for success.

I must mention from the outset that this subject has aroused my interest due to the possibility of applying an imaginative evaluation game to the new concept that is under development and implementation, including by the Romanian Armed Forces – the *multi-domain operation*, thus aiming to draw conclusions that lead to a coherent vision of defence in both national and allied contexts.

This aspect is particularly important because the end goal of implementing a concept is to produce capabilities that can effectively apply it. Thus, identifying how a concept will be adapted and implemented will subsequently involve developing new capabilities, a process that requires sustained financial effort and may lead to delays at the national level, as it largely depends on what the defence industry can produce.

The ideal in the field would be accelerated capability development while reducing costs (Transformer, 2011), but these aspects depend on the nature and technological level of the defence industry. In optimal conditions, a developed defence industry could meet 80% of requirements in a relatively short time (e.g., 2 years) or 100% over a longer period (e.g., 10 years) (Ib.), indicating the timeline for concept implementation.

I have mentioned these elements, which can be considered research limitations, to remain grounded in reality and avoid creating the false impression

that the research tools described in this article will be implemented and utilized according to their general description and the fixed (indicative) timeline for execution.

Furthermore, the fact that the defence industry is an important element in the concept implementation process obliges us to limit our analysis to an ideal case, which cannot always be put into practice. However, it can offer us a guide to best practices and a basis for further analysis applied in real conditions, which depend on how the defence industry will develop as well as on possible arms and military technology acquisition programmes from countries with a higher level of technologization.

Therefore, my intention in this article is to describe the types of assessment games used at the NATO level, both as an Alliance and in member and partner states, to underscore the importance of the experimentation process in capability development. Once the experimentation process is described, I will elaborate on the Concept Development Assessment Game (CDAG) to serve potential future applications in different situations. I mention that I have applied this tool in the case of the multi-domain operation concept, obtaining elements that could complement future developments of the concept and implications for capability development, especially for the Naval Forces.

The research methodology has involved literature review aimed at identifying and synthesizing existing research on imaginative assessment games and their use in capability development, as well as comparative analysis in relation to the effectiveness of various types of games (CDAG[1], DTAG[2], CAPAG[3]) in the capability development process.

THE ROLE OF THE TABLE TOP ASSESSMENT GAMES IN THE EXPERIMENTATION PROCESS

One of the main goals of table top assessment games is to enhance decision-making skills and prepare participants for real-world challenges. By engaging with realistic scenarios, these games allow individuals and teams to explore the implications of their decisions in a risk-free environment. It helps identify weaknesses or gaps in planning, refine quick thinking, and improve adaptability.

[1] Concept Development Assessment Game.
[2] Disruptive Technology Assessment Game.
[3] Capability Assessment Game.

The benefits of table top assessment games include:

- Risk reduction: By practicing reactions to different scenarios, organizations can identify and mitigate potential risks before they occur.
- Improved communication: They promote open communication among team members and between different departments, encouraging collaboration.
- Creative problem solving: Players are often challenged to think unconventionally and explore innovative solutions, enhancing their problem-solving skills.
- Performance evaluation: These exercises provide a platform for assessing team performance and individual contributions, highlighting strengths and areas needing improvement.
- Preparedness and readiness: They prepare teams for unforeseen events, improving readiness and ensuring smoother operations during real crises.

Table top assessment games have a wide range of applications. In the military, they are used to simulate combat scenarios and evaluate tactical decisions. Emergency management organizations use them to prepare for natural disasters, pandemics, or other crises, ensuring effective coordination and response. In business, these exercises assist in developing strategies for managing market changes or cyber threats.

I believe they can be considered useful tools for improving strategic thinking, preparedness, and collaboration. As the complexity of the security environment increases, these exercises offer a practical method for anticipating challenges and creating effective responses. By simulating real-world scenarios in a controlled environment, these types of games enable participants to learn, adapt, and optimize their strategies, ultimately leading to more resilient and responsive organizations.

Although there are numerous approaches to experiments conducted in the defence field, considering our country's NATO membership, I will present the Alliance's perspective on table top assessment games (TTAG): CAPAG, DTAG, and CDAG.

Thus, since table top assessment games aim to assess future capabilities by creating interaction between concept developers, field experts, defence industry representatives, planners, and military personnel who will implement the agreed concepts (Collins, Hasberg, 2018-2021, pp. 236-237), I consider that conducting such games, even under participant-limited conditions, can represent a starting point for understanding the transformations expected to occur in the military system.

Moreover, by conducting such cost-free experiments, the risk of investing large sums of money in capabilities before they are presented to those who will have to manage them is reduced (Collins, Hasberg, p. 237) (the military).

The TTAG in the capability development process, a process that is very complex both nationally and, notably, within NATO, involves difficult problems and sometimes leads to solutions that are hard to understand, positioned between brainstorming and simulation (Ib.).



Figure 1: TTAG place in the experimentation process (Ib.)

From the presented information, we observe the necessity of addressing sufficient issues before inputting data into a system, data upon which simulations might be based. That is why I consider the conduct of such games necessary, as they compel participants to ask sufficient questions to identify needs regarding both capability development (CAPAG) and the use of technology in its early stages of development (DTAG), as well as concepts under development (CDAG).

It should be noted that in NATO's reference document (ACT, Concept Development and Experimentation, 2021), CAPAG is not presented as a method of experimentation and analysis.

It seems, as stated by the author of the CDAG and DTAG manuals, that these types of imaginative games have naturally emerged as a result of lessons identified in the field of concept development and experimentation over the past 10 years (Collins, Hasberg, p. 238).

In addition to the previously mentioned points, the fact that:

- TTAG has been applied in various fields – from space deterrence to operational logistics;
- The results obtained from the games have led to the improvement of certain concepts (validity testing);
- The NATO process for concept development and implementation (CD-E) is suitable for using TTAG (Ib., p. 237),

has prompted me to study these experimental methods in depth and apply them to the multi-domain operation concept.

To understand the timeline, the purpose of each imaginative game, the extent to which they are suited to the capability development process, and the input factors necessary for their execution, I consider the figure presented in the study by Sue Collins and Marcel-Paul Hasberg to be relevant *(figure 2)*.

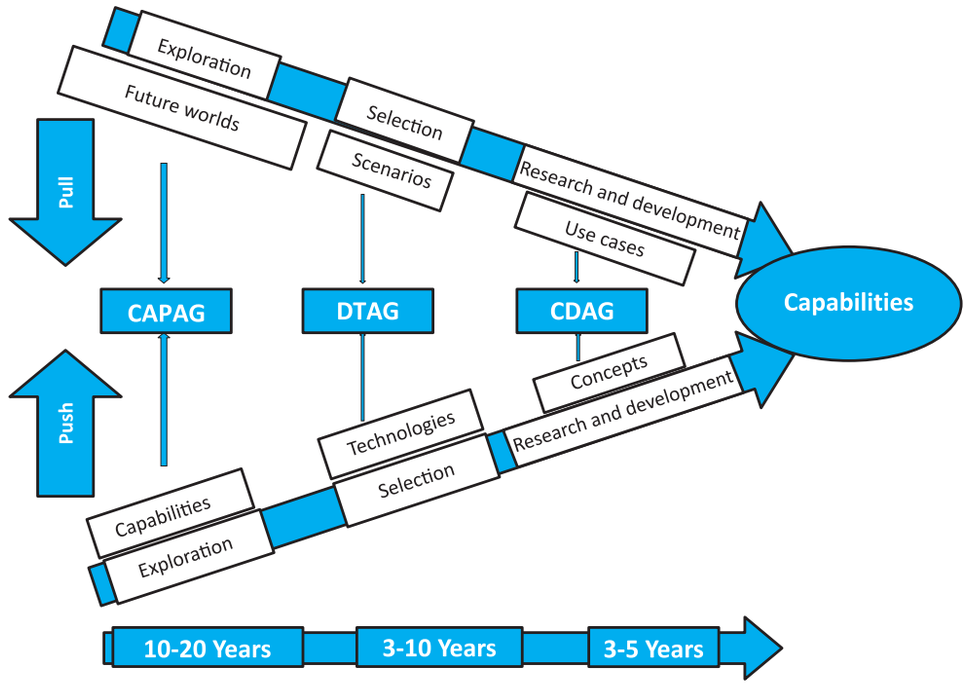


Figure 2: The three types of assessment games within the Capability Development Process
(Collins, Hasberg, p. 239)

To understand the referenced figure, a few clarifications from the cited study are necessary:

- The arrows labelled *"extract"* and *"contribute"* represent different influences on military planning. *"Extract"* refers to aspects over which the military have very little influence, such as the future operating environment and scenarios in which they will have to operate. *"Contribute"* refers to factors over which the military have influence and requires a strategic decision, such as which capabilities are needed in the future, what technologies need to be developed, and what concepts need to be developed (these are the input factors).

- The figure also presents the indicative timeline for conducting each type of game: CAPAG for long-term planning, to explore future capabilities; DTAG for selecting technologies of interest for development; CDAG for researching, testing, and validating a concept.
- It is not necessary for the three types of games to be conducted sequentially; certain stages can be skipped, or they can be carried out within a different timeframe than that presented in the figure (Collins, Hasberg, pp. 238-239).

Having clarified the role and place of each assessment game, I will now detail the Concept Development Assessment Game (CDAG) to clearly understand what it entails, in which variants it has been conducted so far, and to potentially serve as a useful tool for those interested in its application.

CONCEPT DEVELOPMENT ASSESSMENT GAME – APPLICATION, DESCRIPTION, RULES

The Concept Development Assessment Game (CDAG) was developed in 2009 by the Allied Command Transformation in collaboration with the Netherlands Defence Research Organization, aiming to create a structured framework that combines the intellectual freedom of brainstorming with analytical rigour and control to obtain relevant results that contribute to the development, refinement, and evaluation of concepts (Feckler, 2011, p. 2).

To describe the purpose, applicability, and methodology of CDAG, I have corroborated information regarding the conduct of the imaginative game from sources that directly reference it (ACT, Concept Development Assessment Game Handbook, V4.1, 2014; Collins, Hasberg, 2018-2021) with the NATO Manual (ACT, Concept Development and Experimentation, 2021), which generally describes concept experimentation and development.

Thus, CDAG is a qualitative method of experimentation applied to test and develop conceptual documents, focusing on intellectual challenges and discussions regarding the document under analysis (ACT, Concept Development and Experimentation, 2021).

It should also be mentioned that the cited document indicates three elements that combined would constitute CDAG: brainstorming, simulation, and the red team (a team designed to challenge the blue team that tests a subject), which somewhat contradicts the place of TTAG in the experimentation process, presented earlier in *figure 1*.

Nonetheless, the game primarily focuses on challenging discussions related to the proposed document or subject by allocating tasks and approaching the subject from different perspectives (Collins, Hasberg, p. 243).

A simplistic[4] presentation of the game's methodology is as follows:

- The document/subject/concept is simplified by extracting relevant elements or selecting certain parts to be described in concept cards.
- The technology that might enable the application of the concept can be described in technology cards to avoid using specialized systems or simulations.
- The game is conducted in rounds, each round being independent, which provides flexibility (usually six rounds conducted over three days – the duration and number are flexible).
- Each round includes an initial briefing, a team planning session, and discussions according to the tasks set (in which all teams participate).
- The operational context is ensured through scenarios, specific tactical situations called vignettes[5], and role-playing games, which should present a low level of detail to be understood in a short time (ACT, Concept Development and Experimentation, ib.; Collins, Hasberg).

I believe that this information is well synthesized in a presentation conducted by one of the game's co-authors (Netherlands Defence Research Organization) *(figure 3)*.

In addition to the aforementioned points, a questionnaire can be used both at the end of each round and at the end of the game – questionnaires that aim to evaluate not only the team's outcome and the conceptual document but also the broader domain encompassing the subject (ACT, Concept Development Assessment Game Handbook, V4.1, 2014).

I believe it is important to also mention the reasons why this type of game is used:

- It is useful for complex, hard-to-quantify issues that cannot be addressed through mathematical solutions (solutions are not obvious to participants or concept developers);
- It has an open format that facilitates the creation of a community of experts;
- It reduces the risk of incorrect concept implementation;

[4] For details, see Allied Command Transformation, *Concept Development Assessment Game Handbook*, V4.1, 2014.
[5] Specific situations created within the scenario to test the participants' mode of action.

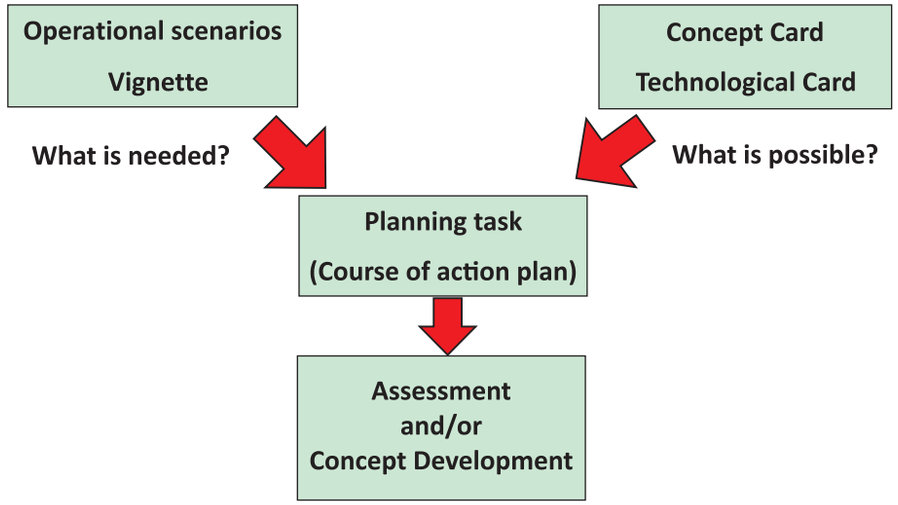


Figure 3: CDAG General Setup (Elst)

- It is a flexible tool – adjustments can be made during the game;
- It can be used as a learning method on the addressed topic (ACT, Concept Development Assessment Game Handbook, ib.).

Participants in the game are the concept developers and/or future users of the concept/document that will present the concept:

- Typically, three teams of six to eight participants will assume roles according to the proposed scenario;
- Analysts who collect data based on discussions, both in team work and plenary sessions (questionnaires can also be issued to fulfil this purpose);
- Specialists who can advise players;
- A moderator to facilitate plenary discussions and ensure that the game's rules are followed (Ib., p. 1).

To have an overview of what a game round entails (briefing, teamwork, questionnaire, and feedback), I believe a succinct description of the constituent elements is necessary.

- *The briefing* involves the following activities:
  - Presenting the scenario to create the operational context;
  - Presenting the vignette for each round;
  - Team tasks;
  - Team roles (Ib., pp. 6-17).

- *Teamwork* involves the following main activities:
  - Teams fulfil tasks using concept and technology cards;
  - Analysts observe discussions, ask questions, ensure concept cards are used, and record discussions and team results;
  - Consideration of questions from the *questionnaire* to be answered at the end of the round;
  - Guidance can be sought from the moderator and concept presenters (Ib., p. 17).

Plenary discussion and questionnaire completion have the following objectives:

- Data collection;
- Presentation of task results;
- Questions from members of the other team;
- Questions from concept presenters, the moderator, and analysts;
- Questions focus on evaluating the team's product, concept evaluation, and integrating the subject into a broader subject (Ib., pp. 17-18).

Feedback is essential for concept presenters to ensure that participants agree with elements identified during the round and to correct any errors (Ib., p. 19).

Through the presented information, I have tried to provide an overview of what the concept development imaginative game entails, which, as mentioned in the introduction, I consider can serve future research.

I believe it should also be noted that the CDAG manual recommends that if game developers lack experience in organizing such events, previous models or best practices in conducting such games are recommended.

Thus, considering that I have participated in such events but have not been in the position to organize such a game, I have studied how they have been applied to date.

For example, one such game, addressing a smaller-scale issue yet relevant in the maritime field, is the one presented by Jenni Gotzi and Karl Skoog in the study *"An Adapted Version of the Concept Development Assessment Game – Experiences from the Swedish-Finnish Naval Task Group Discussions"* (Gotzi, Skoog, 2015).

CONCLUSIONS

Table top assessment games prove to be essential tools in the capability development process, allowing for the testing and refinement of strategies in a controlled and risk-free environment.

These exercises significantly contribute to enhancing decision-making skills by exposing participants to complex and diverse scenarios, thus improving their ability to adapt and react in real situations.

Successful implementation of assessment games requires collaboration among experts from various fields, such as concept developers and defence specialists, ensuring an integrated approach to capability development.

These games play a crucial role in identifying training deficiencies and promoting organizational learning, helping align strategies and processes with the dynamic requirements of the security environment.

Although table top assessment games offer multiple benefits, their conduct is not without challenges, such as the need to adapt the games to the specific requirements and constraints of each organization or scenario.

From the military context to higher education and corporate strategies, assessment games demonstrate versatility, being used to stimulate creative thinking and innovative problem-solving across various domains.

However, it should be noted that success in implementing new concepts is closely linked to the development and capacity of the defence industry, whose involvement is crucial for achieving viable and effective capabilities.

BIBLIOGRAPHICAL REFERENCES:

1. ACT (2014). *Concept Development Assessment Game Handbook, V4.1.*
2. ACT (2021). *Concept Development and Experimentation.*
3. Collins, S., Hasberg, M. (2018-2021). *Table Top Assessment Games in Concept Development and Experimentation*. *ACT, Advances in Defence Analysis, Concept Development and Experimentation: Innovation for the Future*.
4. Elst, N., van (n.d.). *Concept Development Assessment Games – Description, use and some examples,* www.expertsinuncertainty.net: https://www.expertsinuncertainty.net/Portals/60/Madrid_presentations/VanElst.pdf?ver=2017-12-20-155117-357, retrieved on 2 October 2024.
5. Feckler, D. (2011). *ACT Employs Analytical War-Game. The Transformer, Bi-Annual Publication of Allied Command Transformation,* vol. 7, no. 2, p. 2.
6. Gotzi, J., Skoog, K. (2015). *An adapted version of the Concept Development Assessment Game – Experience from the Swedish-Finish Naval Task Group Table-Top Discussion.*

7. Transformer (2011). Brigadier General Fungo, *Discusses Concept Development and Collaboration with Industry. The transformer, Bi-Annual Publication of Allied Command Transformation,* vol. 7, no. 2, p. 2.

THE EVOLUTION AND ROLE OF COOPERATION FOR ORGANIZING AND CONDUCTING MILITARY OPERATIONS

Colonel (r.) Assistant Professor Iurii CIUBARA, PhD

"Alexandru cel Bun" Military Academy of the Armed Forces, Chișinău, Republic of Moldova

DOI: 10.55535/RMT.2024.4.11

This article analyses the role and importance of the concept of cooperation in the preparation of military operations and battles, based on studies focused on the conduct of combat actions and command exercises. The evaluation of the conclusions and lessons learned in the military field, from a theoretical and practical perspective, highlights that an effective organization of cooperation occupies an essential place in the preparation of military confrontations. Recent experiences in armed conflicts emphasize that neglecting this distinct aspect in planning and executing combat actions can lead to the failure of missions.

The author focuses on the analysis of relevant sources and the elucidation of significant phenomena and aspects related to the mentioned topic. The results of the study, obtained by examining the factual material and formulating ideas based on the lessons learned, will be valuable for the development of national military art. In conclusion, it is emphasized that military experience has enriched military art with new applicative perspectives and teachings, which will continue to be influenced by the development of modern technologies and the evolution of the operational context and means of combat.

Keywords: armed forces; strategy; physiognomy; cooperation; operational art;

INTRODUCTION

The current regional geopolitical context, which is characterized by the escalation of the Russian-Ukrainian armed conflict and the instability in Ukraine, necessitates a re-evaluation of the functioning of the defensive system. This need is manifested by reconsidering the strategies for deploying forces and resources in the defence system. The confrontation between Western doctrines and elements of Soviet military art is highlighted when analysing various military actions observed during the Ukraine War after the Russian invasion. Particularly relevant is how new technologies are integrated into the modern battlefield, forcing both sides to find innovative solutions to achieve a favourable force ratio and gain strategic and tactical superiority in decisive areas.

As is known, the conduct of war has evolved over time under the influence of the development of society, science, and the refinement of technological processes, which have created premises for the new physiognomy of armed conflict. From this point of view, it can be noted that the evolution of the armed combat at the beginning of the 21st century denotes the configuration of new elements, previously almost negligible or having insignificant impact on the theatres of war.

The conflict in Ukraine has brought attention to new combat methods at all levels of military art, causing essential revisions of strategic and tactical concepts. Analysing conceptual innovations in aviation, cruise missiles, armoured technology, and unmanned aircraft (drones), we note that these technologies are being used intensively by both sides for both surveillance and attack. These developments have not remained without consequences, contributing to the transformation of the physiognomy of the armed struggle and bringing an innovative character to the preparation and conduct of military/combat operations. Both sides must adapt to a particularly difficult situation when using new means in the context of the modern battlefield, which is characterized by extremely varied conditions and situations. We also observe competition in conducting combat actions, in which the forms and contents differ depending on the quality of the forces involved. So far, none of the countries involved in the conflict can be considered a winner and cannot argue that it has fully achieved its political objectives.

At the same time, it can be found that military art evolves in close accordance with technical and scientific progress, which influences the way the armed struggle

is conducted both now and in the future, at the strategic, operational and tactical level. The objectives of the military actions at strategic and operational level are pursued and realized by groups of forces with strategic and operational value, through complex military operations. At the tactical level, the actions are carried out in the form of direct fights.

Therefore, the dynamics of the evolution of military actions requires an evaluation of this conflict, in order to extract the most relevant lessons that can be integrated in the military training of the national armed forces personnel. These lessons are essential and will continue to represent a major interest in the training and preparation process for the deployment of future military actions.

CONSIDERATIONS FOR THE ORGANISATION OF COOPERATION

Following the study and analysis of the history of wars presented in the literature, the essential role of cooperation in organizing and conducting combat actions is highlighted. We should mention that the American military historiography from the period before the Second World War elucidated the concept of cooperation only in general terms, and as a result of these gaps, American forces suffered significant losses in the first phase of the Second World War.

In contrast, the British literature during the war addressed the principle of cooperation in more detail, but its practical implementation was not always appropriate to the situation on the ground. As regards German historiography, the regulation *"The Troops Management"* emphasized cooperation as one of the fundamental tactical principles. In the orders of the command of that period it was strongly recommended to use all necessary resources to ensure effective coordination and punctuality in the performance of missions (Frieser, 2010, p. 370).

In this context, Russian historiography makes solid arguments in favour of the emergence of the first elements of cooperation between different services during the First World War. The development of those elements was intended to study, plan, and coordinate cooperation between military units in operations, a concept that was tested and refined in subsequent conflicts (Воробьёв, 2002, p. 129).

The Second World War, characterized by much greater mobility and military actions of considerably greater proportions than those in the First World War, highlighted even more clearly the importance of an effective system of cooperation. During that time, the notion of *cooperation organization* became a central element in planning and conducting military actions, being thus regulated and detailed in the official military documents. We believe that the development of those rules and procedures was essential for the success of complex military operations,

where synchronization between different branches and units became a decisive factor in achieving superiority on the battlefield. Thus, cooperation was no longer an abstract concept, but a fundamental tactical principle, applied at all levels of command and considered vital to achieving strategic objectives.

During the Second World War, the theory and applicability of the organization of cooperation was significantly improved, bringing this concept to a new level. Cooperation became a key element in the preparation and deployment of combat actions, directly contributing to the achievement of operational objectives. The evolution was determined by the need to adapt the military structures to the new realities of the battlefield, in the context of continuous improvement of military technologies. The armed forces' mobility was enhanced by the introduction of mechanized troops and armoured vehicles, and the processes of action evolved to match different types of combat. Thus, the theory of cooperation had to integrate those new trends and provide effective solutions for the rapid and precise coordination of military actions on multiple fronts (Ib., p. 145).

After the Second World War, as well as in local military conflicts, military science, especially military art theory, continued to evolve at the pace of technological progress. It remained an integral component of the preparation and conduct of military actions, being always adapted to the new realities of the battlefield. The modern means of striking and firing have been used in increasingly effective ways, thanks to the adoption of innovative or even previously unknown action processes. In this context, the new military equipment has required clear and well-established procedures for use in combat. These procedures have required a reassessment of the way cooperation is organized, resulting in a new vision that integrates modern resources and technologies into the cooperation system to maximize battlefield efficiency. Thus, the rapid evolution of military means and the complexity of modern operations have created a framework in which cooperation is no longer only an option, but a strategic necessity for the success of military actions.

The new conditions under which military actions are designed and carried out oblige us to carefully re-evaluate the action processes of the forces and means involved. The physiognomy and content of these actions are not constant, but vary depending on the level of technological development of the armed forces and the specific conditions under which the fight is conducted. Determining factors of military action, such as the enemy, geographical space, time available and the ratio of forces, together with the available means, must always be taken into account in the planning and execution process.

An essential element in the conduct of military operations is the principle of continuity. This principle emphasizes that military actions are not isolated events, but are part of a constant process of adaptation and evolution. Continuity means not only maintaining a strategic link between the different stages of a military campaign, but also the ability to integrate past experiences into future planning. Thus, the armed forces must be prepared to adjust their tactics and update their equipment in order to respond effectively to ever-changing scenarios.

The application of the principle of continuity in the organization of military cooperation requires uninterrupted coordination between all elements of force. It guarantees that, regardless of the developments on the ground or the changes in the dynamics of the confrontation, cooperation remains a constant factor, which maximizes the efficiency of the actions. In this respect, the command must be able to anticipate and adapt cooperation plans, ensuring a solid link between the stages of preparation and conduct of operations. This continuity is vital for maintaining operational momentum and avoiding discontinuities that could give the enemy decisive tactical advantages.

The conclusions drawn from the analysis of the evolution and transformations in the conduct of military battles and operations have played a significant role in redefining the strategic planning process. Technological, tactical and strategic transformations have resulted in essential adaptations in military art, bringing profound changes in the way operations are conceived and carried out on the battlefield. These mutations are based not only on technological developments, but also on the experience gained in modern conflicts, which demonstrate the need for dynamic and flexible planning, able to respond quickly to ever-changing circumstances.

Returning to the division of military art in the three distinct levels – strategic, operational and tactical, we can emphasize that, despite the differences between these levels, certain fundamental elements remain constant, such as space and t ime factors. These two coordinates play a significant role in determining the success or failure of a military operation, regardless of the level at which it is conducted. Space defines the location and mobility of forces, and time influences the ability to react and synchronize, essential aspects in the context of a modern war, characterized by the rapidity of changes and the complexity of operations carried out simultaneously on multiple fronts. Starting from these considerations, the preparation and management of military actions at each of the three levels are carried out according to specific laws, principles, rules and procedures, which vary depending on the scale and complexity of the operation. At the strategic

level, the focus is on long-term planning, resource coordination and setting major goals. At operational level, it aims to manage resources and coordinate units to ensure continuity and efficiency in achieving strategic objectives. Finally, at the tactical level, the focus is on concrete implementation of plans through actions on the ground, where space and time factors are decisive in gaining advantage over the enemy. Thus, each level operates under distinct constraints and opportunities, but the interdependence between them ensures the complex success of military actions.

In the context of armed confrontations, any military action requires multilateral assurance, including the creation of optimal conditions for a thorough preparation of each operation, the strengthening of force groups and the maintenance of an adequate combat capability. This training requires both effective coordination of available resources and rigorous control of military logistics so as to achieve operational objectives. Changes in the nature and structure of armed conflicts have required a deep re-evaluation of the procedures for the transition to various forms of combat, adapting them to new strategic and technological realities.

From the theoretical-applicative perspective, a significant example of these developments is the phrase *organization of cooperation*, which occupies a central place in the preparation and conduct of combat actions. Cooperation between the various units and branches involved in a military operation not only optimises the coordination and efficiency of forces, but also plays a crucial role in the adaptability and flexibility of military actions. The historical study of wars and lessons drawn from past experiences underscores the importance of cooperation as a decisive factor in the success of modern military operations.

Moreover, the applicability of the concept of *cooperation* has been demonstrated in all areas of military art, being illustrated by the way in which troops belonging to different branches collaborate in order to achieve common objectives. This strategic principle has played a decisive role in achieving success on the battlefield, facilitating the synchronization of forces and multiplying the combined effect of various military resources. Thus, the effective organisation of cooperation continues to be an essential pillar in the planning and execution of military actions, having a direct impact on the outcome of armed conflicts.

According to the military lexicon, the concept of cooperation is defined as *"Activity that ensures the coordination of actions of all forces participating in combat (operation), in time, space and missions, and, for the purpose of concentration and summation of their efforts for the performance of a joint combat mission".* (Military Lexicon, 1994, p. 111).

Military art has its share of controversy and debate, much like any scientific field. Testing and applying certain provisions and theories in real combat contexts is the only way to demonstrate their validity. The dynamic nature of war, in which external and internal variables are constantly changing, creates a framework in which even the most robust principles must be adapted and reassessed based on the results obtained on the ground. Thus, the theory becomes effective only when it can be successfully translated into practice, and its applicability must be proven by means of concrete results of military operations. In this context, a current debate within the military theory is to elucidate the organization of cooperation in the preparation of military actions, a problem that has gained increasing importance in recent literature. Organizing cooperation involves effectively synchronizing resources and forces to maximize the effect of military operations, but this approach requires constant review as new technologies and combat strategies emerge.

Mention should be made that, in the literature, the notion of coordination is a fundamental element, representing the third pillar in the tertiary stage of preparing a military operation. The notion of coordination brings an important clarification in the dynamics of the organization of forces, highlighting the fact that the success of an operation does not depend only on the readiness and execution capacity of each actor involved, but also on how these actors manage to collaborate and adapt to the changes occurred during the conflict. In this context, coordination is not a mere technical mechanism, but an essential component, which ensures the overall cohesion and efficiency of all the resources involved in the action, transforming strategic potential into a concrete reality on the battlefield.

From an etymological point of view, the notion can be analysed through two essential concepts: coordination and cooperation, within the framework of contemporary military planning, these two concepts, treated differently, reflecting varied approaches in the armed forces of modern states. Semantic and conceptual differences between coordination and cooperation often create significant impediments to the preparation of military operations and the effective organization of cooperation between various units and branches. In the absence of precise clarification of these concepts, the planning process risks becoming inefficient, leading to a misunderstanding of how these elements integrate into a military operation.

Starting from this semantic dissonance, we appreciate that conceptual adjustments and clarifications are needed to ensure an effective operationalization of the notion of military cooperation. Currently, a gradual departure from

the classical definition of cooperation is noted, which can lead to difficulties in applying this concept in real military contexts. In this context, our approach is more methodological and didactic, focusing on the need to provide a clear and coherent theoretical framework, facilitating the implementation of cooperation in the planning and conduct of military operations.

Romanian specialists support the idea of conceptual division between coordination and cooperation, although, in the past, in the Romanian military theory, cooperation was considered a stand-alone principle in the armed struggle. The justification for this perspective can be found in the *"Doctrine for Land Forces Operations"*, a fundamental document that was modelled after the main military doctrines of NATO member states, but adapted to the specific of the Romanian army. This doctrine reflects the need to combine own military traditions with the most advanced international practices, constituting a coherent body of knowledge and rules that meet the modern challenges of the battlefield (F.T.-1, 2004).

In a different manner, the mentioned problem is dealt with by Russian military specialists, who exclude the existence of division, finding that, in principle, cooperation is self-contained (Воробьёв, p. 119). It is also considered that one of the important problems of the theory of military art, faced by the applicative part, is represented by the ways of organizing and conducting military actions in the current conditions of the battlefield. We believe that the cooperation of forces and means between different branches is one of the important elements in the preparation and planning of combat actions that are embedded in the spectrum of key elements regarding the characteristics of the orographic system elements, time conditions and weather conditions.

However, to elucidate the concept in terms of the importance and delineation of cooperation from the theoretical-applicative point of view in relation to the levels of military art, we will rely on the content of relations of interaction and interdependence between the components of military art. Therefore, the existence of relations of subordination between the levels of military actions is a necessity dictated by the needs of the battlefield, through which they are manifested, determining the level of activity of the structures in order to organize and maintain cooperation.

In our opinion, cooperation consists in coordinating the combat actions of heterogeneous forces from different military services, branches, as well as neighbouring forces or forces from the relevant ministries over time, space and on missions, in order to successfully carry out joint missions.

Therefore, the *essence of cooperation* lies in the coordination of the actions of forces from different branches in the interest of infantry troops, tanks, sub-units and units acting in the main direction of effort or in the main direction of offensive.

The importance of cooperation lies in the fact that it allows the use of combat capabilities of large units and units, arising from the capabilities of the armament in the inventory. Through cooperation, the vulnerable points of some forces and means complement each other's strong points, thanks to which a significant superiority is achieved in the total action in terms of the effect on the enemy.

Therefore, the *purpose of cooperation* is to make the most effective use of the combat power of the forces of different services and branches involved in combat, concerned with the accomplishment of the mission. Thus, the conduct of the armed struggle provides for the participation of various forces from different services and branches, having combat properties and capabilities that impose new requirements in terms of the organization of cooperation.

In this context, within the framework of national military science, the organization of the cooperation system must be carried out in accordance with essential fundamental principles: *continuity, stability* and *flexibility*. These requirements are essential for ensuring an efficient and adaptable cooperation system in various military scenarios, reflecting both the need for fluid coordination and the ability to react quickly to changes in conflict dynamics. We will present in detail the principles mentioned, as follows:

❖ *Continuity of cooperation* is achieved through permanent knowledge of the situation, maintaining a high level of training of forces, for carrying out missions in a complex situation, by implementing the processes of organizing and improving the system of cooperation in the fight, as well as by ensuring the system of sound management and communication.

❖ *Stability of cooperation* implies knowledge of the real situation, maintaining the capacity of the created system and operating under conditions of use of the means of destruction of the opponent.

❖ *Flexibility of cooperation* lies in the ability to adapt quickly to any situation. It is achieved by taking appropriate measures to change the situation, specifying and presenting new decisions, sub-unit missions, and ways of cooperation.

Thus, the effective organization of military cooperation, in accordance with the principles of continuity, stability and flexibility, is essential for the success of modern operations. This holistic approach ensures both the resilience of the command-and-control system and the ability to adapt to a constantly changing operational environment, which is a strategic advantage in contemporary conflicts.

In military science, the *principle of cooperation* is manifested by the diversity of military actions, which address numerous applicative challenges related to the conduct of armed struggle. These challenges include various tactical forms and processes aimed at increasing operational efficiency and ensuring success in combat and operations. The effectiveness of military actions is closely related to the adaptability to constant changes in the battlefield, as well as the continuous improvement of weapons and combat technique. In this respect, establishing and maintaining adequate coordination between the various elements involved in the operations are crucial to achieving strategic and tactical objectives.

The achievement of these objectives is becoming increasingly important in the current context, where the armed forces involve a diversity of structures and means from different units and military subdomains. It underlines the need for effective cooperation, not only between own forces, but also between those coming from other structures or alliances. Without precise and integrated coordination, loopholes may arise in the conduct of actions, which can significantly reduce the operational efficiency and the ability to respond quickly and decisively to the challenges of the battlefield.

The experience gained in recent armed conflicts gives us clear evidence that a commander's lack of tactical skills is becoming evident especially in his failure to effectively organise and implement cooperation in operations. Cooperation is an essential test for a commander's ability to coordinate multiple elements in a coherent and effective manner, and without such ability, the success of military operations can be seriously compromised.

The achievement of specific aspects related to the effective organization of cooperation and the rigorous application of operational requirements in the course of a military operation, in the temporal, spatial and tactical dimensions, is a fundamental responsibility of the commander and the staff of the respective echelon. Managing these issues is essential to ensure strategic and tactical success in combat through effective integration of available resources and forces.

The experience gained in recent conflicts, including the war in Ukraine, has shown that one of the main tasks of the command is to concentrate efforts and coordinate actions between the various land, air and anti-aircraft units. This coordination aims to achieve common goals, such as the decisive neutralization of the enemy and the continuity of military operations. The success of an operation depends on the ability of the forces to maintain constant pressure on the enemy, through a series of coordinated actions, which destabilize the reaction capacity of the opponent (https://re-russia.net/review/279/, 2023).

In this context, the organization of cooperation becomes a very important component, derived from the central importance of the purpose of the operation. It involves careful analysis of the actions and means available at the upper echelons, as well as accurate anticipation of the movements of the enemy. In order to ensure operational success, it is essential to highlight the clear sequence of activities carried out by the commander and the staff for the effective coordination of the resources and forces involved.

We note that the system of cooperation, having a centralized character, gives the commander a primordial role in the management and coordination of all actions, and the final responsibility for the success of the operation lies, thus, with the commander, who must ensure that all resources are allocated and optimally managed to maximize the strategic effect and to successfully carry out the mission. This centralization of coordination not only simplifies the decision chain, but also ensures a clear continuity in the implementation of operational plans, being essential for coherence and efficiency in the conduct of modern military operations.

Thus, the initial data for the organization of the cooperation are: the mission received and the specific conditions for its execution; the provisions of the upper echelon on the organization of cooperation. Therefore, the decision of the commander constitutes the basis for the organization of cooperation.

We emphasize that, depending on the situation created and the form of action, the work of the commander on the organization of cooperation, having a mutual connection, can be divided into *three stages*:

- *the first* is determined on the basis of the appropriation of the primary mission and the analysis of the situation: the commander decides it and determines the main problems of cooperation;
- *the second* is setting the missions on the alignments, time and variants, the procedures for their execution and the directions of action; instructions on cooperation are given;
- *the third* is the direct activity of the commander and the staff in organizing cooperation, which is specified in the field or on a map.

From the experience gained, it follows that the organization of cooperation within military operations involves an essential activity, aimed at dividing combat actions into distinct moments and structuring detailed operational scenarios. These scenarios must take into account the dynamics of actions of both own and opponent troops. Therefore, the effective coordination between different phases of the operation becomes crucial to ensure a rapid and adaptive responsiveness, depending on the evolution of the situation on the battlefield.

Specifically, the main challenges in organising defence cooperation include: identifying and clearly defining actions and activities that take place over the entire depth of the combat device; managing the reaction time for the enemy passing over defensive alignments; efficiently organizing the fire system and defensive dams on the offensive directions of the enemy. Defence-switching variants should also be considered, depending on different missions and tactical scenarios, in order to maximize resilience and response capacity.

The organization of cooperation, based on possible variants of action of the enemy, involves the establishment of flexible combat modalities and procedures, adapted to the operational context. It is also essential to implement a single signal system that facilitates the concentration of efforts at critical moments, ensuring optimal synchronization between the forces engaged and the successful fulfilment of the mission received.

Within this framework, a key aspect of cooperation is the ability to compensate for the inadequacies of one branch by using other branches, thereby ensuring tactical complementarity. Precisely predicting the evolution of the tactical situation and avoiding failure in combat are integrated into the complexity of the problems that the commander and the staff must solve. These challenges require not only a good understanding of the operational context, but also an impeccable execution of strategic plans, based on rigorous and flexible coordination of all available forces.

Within the offensive, cooperation issues are determined on the basis of assigned missions, alignments and key moments, being detailed according to the depth of the immediate mission. This process includes planning to move to the *offensive from the movement*, establishing the succession and the time required to cross the initial alignments, the effective deployment of the offensive action and the optimal time to trigger it. At the same time, the specific missions and the time necessary to carry them out, as well as the time of preparation of the forces for launching the offensive, are precisely determined.

In the event of a transition to the *offensive of direct contact with the enemy*, the additional indication shall be both the time and the order of regrouping or replacing the units involved, and, to ensure continuity of actions and avoid losses caused by lack of synchronization. This careful organization allows to maintain a constant pace of operations and quickly adapt to the changes in the battlefield.

The methods of organizing cooperation under the current conditions are varied and flexible, being determined mainly by the specificity of the operational situation, the level of training of the forces and the experience of the commanders involved. Contextual factors such as technological evolution, enemy nature and geographic

conditions influence the way cooperation is planned and implemented, requiring an adaptive and innovative approach to ensure the success of offensive actions (Watling, Reynolds).

CONCLUSIONS

Of the many challenges of military art, organizing and maintaining cooperation for the annihilation of the enemy occupy a central place, being a field that requires creative and innovative solutions, not only from a theoretical perspective, but also from a practical one. Cooperation is both a matter of technical coordination and a dynamic process, involving adaptability and continuous adjustments depending on the evolution of the situation on the ground. Maintaining cooperation during military actions is a critical mission for the commander, whereas the inherent changes during operations frequently require the modification of the original plan in order to remain effective and relevant in the face of an unpredictable enemy.

In order to ensure the continuity of cooperation during the conduct of military actions, the commander must constantly monitor whether the actions of subordinated units are in line with the original plan and whether they remain synchronised with the strategic objectives set. This active oversight is essential to prevent uncontrolled deviations from the operational plan, which may jeopardise the overall success of the mission. In a modern struggle, where dynamism and unpredictability are the order of the day, the ability to maintain the coherence of subordinate actions becomes a test of the quality of military leadership.

More than ever, in the current context of increasingly complex and interconnected conflicts, the organization and maintenance of cooperation between all forces and means involved in a military operation is a critical node in the chain of missions of the commander and the staff. Whether land, air, naval forces or logistical support elements, the success of an operation depends crucially on the synergy between these elements, which underlines the importance of crack-free coordination. The essential role of the commander is to coordinate these elements efficiently, in order to transform the operational potential into a concrete success on the battlefield. As the above-presented aspects show, the system of cooperation has evolved considerably throughout the history of military art, reflecting major changes in technology and tactics of war. Much of the knowledge gained on the application of this concept remains relevant today, providing valuable lessons that guide the planning and execution of contemporary operations. On the other hand, as military technology and the operational environment continue to evolve, the cooperation system must also adapt to meet new challenges.

Therefore, the experience of the past should be seen not only as a solid historical basis, but also as an essential guide to the future development of military strategies and tactics. It indicates the necessary directions of improvement to meet the modern challenges of war and maximize the efficiency of armed actions.

BIBLIOGRAPHY:

1. Agud, I. (1994). *Lexicon military/Military Lexicon*. Chișinău: Editura Saca.
2. Воробьёв, И. (2002). *Тактика-искусство боя, Москва*, военное издательство 2002.
3. Frieser, K.H. (2010). *Mitul Blitzkrieg-ului. Campania Wehrmachtului în vest. 1940*. Bucureşti: Editura Militară.
4. F.T.-1 Doctrina operațiilor terestre/Doctrine for Land Forces Operations (2004). București.
5. Мясорубка: Тактика России во второй год ее вторжения в Украину (2023), https://re-russia.net/review/279/, retrieved on 22 June 2024.
6. Watling, J., Reynolds, N. *Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine*, https://static.rusi.org/403-sr-russian-tactics-web-final.pdf., retrieved on 22 August 2024.

MASKIROVKA
– THE ART OF DECEPTION À LA RUSSE –

Iulia BORISOV, PhD Candidate
University of Bucharest
DOI: 10.55535/RMT.2024.4.12

Synonymous with disguise, camouflage, diversion and deception, maskirovka is a complex Russian cultural phenomenon, which has already reached the rank of doctrine. The Armed Forces of the Russian Federation have carried forward military theory, doctrine and thinking between the years after the collapse of the Soviet Union and the Russian political-military revival. It is also reflected in the increased importance of diversion in achieving military objectives. Maskirovka is culturally rooted in the Russian mentality and represents a significant component of Russian military operations. This paper aims to analyse the evolution of this phenomenon in Russia, from a military to a political concept, from the Second World War to the invasion of Ukraine in 2014, as well as its psychological implications. Once a means used to gain advantage on the battlefield, maskirovka is utilized in order to create ambiguity and uncertainty in the environment it operates on for freedom of action in achieving the military and political objectives of today's Russia.

Keywords: disinformation; influence; maskirovka; psychological operations; Russia;

INTRODUCTION

Russian military deception is based on a tradition developed during the Cold War by the army and intelligence agencies of the Soviet Union. It is part of USSR's military history, since there already was a Tsarist school of *"deception"* before the revolution, where techniques of interference and action on the enemy were taught. While that school was dissolved during the Revolution, its principles were transposed by the Red Army in its official Field Regulations of 1933. The strategic value of Russian military deception has consistently shown an ability to cause damage and to alter, temporarily or permanently, the thinking of individuals, their perceptions, their emotions and their elements of the communication process in groups where such harmful effects are manifested. The mechanism is simple, using all possible levels and sources of knowledge of behaviour as studied by the great Russian psychologists, for military and political-military actions and, thus, acting on individuals and on the groups and social ensembles they make up and contribute to the success of the action. Influence is an integral part of the action; it is a strategic function.

The Russian doctrine of military deception has evolved significantly starting with the beginning of the last century. It has accompanied ideological revolutions, from the first communists to the end of the USSR, up until the return to the context of the Cold War anew, with Russia returning to the old constants of enclavism and supremacy. Recently, it has been confronted with the emergence and then the evolution of digital technology in particular, which has given it a new face, more generalized, more diffuse and probably more formidable for its targets and victims.

Westerners are generally unaware of its importance. They minimize it, neglect it, and it escapes them beyond a mere superficial knowledge (Smith, 1966, p. 30). Another impediment is the fact that Russian terms are not easily translated into English, French, or Romanian. However, beyond the linguistic difficulty, this is, above all, a matter of difference in culture, in the conception of the world and its equilibrium. The context in which it is implemented is also difficult to understand. It is overwhelmed by Russia's constant, almost paranoid assessment of the potential danger posed by social groups and individuals that compose them, enemies both from outside and from within.

In this context, even though this term first of all refers to the activities and methods of masking and concealment, it has long embraced dimensions other than that of simple military camouflage (Hutchinson, 2004, p. 170). The word, in Russian, literally means *"masking"*, as in covering something with a mask, disguising or camouflaging. In essence, it is the art of deception *à la russe*. *"It is simply designed to keep adversaries permanently off-balance"*, explains Lindley-French (2018) on her blog. It is a generic term today that designates a concept that is "*complex, diffuse, although very well structured, institutionally recognized as officially funded, and carefully planned*" (Smith, 1966, p. 32), in order to establish one of the doctrinal principles of the state. Thus, in general terms, all Russian actions should be hidden as much as possible from the enemy, whether it be real or potential. The intention of a commander, decision-maker, or other leader must always be disguised in order to improve the chances of surprise. And this principle applies simultaneously to all three levels: strategic, tactical, and operational.

Debates in Russia on this phenomenon have focused on the prevalence of the terms *obman* (deceit), *voyennaya khitrost* (military cunning), and *vvedeniye v zabluzhdeniye* (misleading) as synonyms for *maskirovka* (currently in the process of reverting to its original meaning of concealment or camouflage). Russian experts have debated the relevance of the term *maskirovka*. The theorists emphasize that *maskirovka* (with the meaning of concealment/cover-up) is a component of deception (*obman*) and not the other way around. Debates in Russia argue that the term *maskirovka* is vague and illogically groups any form of deception under the Russian term for concealment/cover-up. It has translated *maskirovka* back to its original meaning of hiding/cover-up and led to the use of a more appropriate term to encompass all attempts to deceive under this word. Essentially, the general principles and elements of *maskirovka* are retained, but under a terminology more suited to the exhaustive meaning. Much like *maskirovka*, *obman* is an umbrella term for deception. With the annexation of Crimea by the Russian Federation in 2014, *obman* replaces *maskirovka* in an effort to remain within the currently accepted Russian concept of deception (Thomas, 2011, pp. 113-116).

Russia's understanding of the nature of war, like its conceptualization of deception, has evolved over time. Commonly referred to as the Gerasimov Doctrine or *"New Generation Warfare"*, the Chief of the General Staff of the Armed Forces of the Russian Federation, General Valery Gerasimov, outlined his observations on modern warfare in *Voenno-Promyshlennyi Kurier* (*Military-Industrial Courier*). General Gerasimov, along with other Russian military theorists, made several important observations relevant to the Russian invasion of Ukraine. Gerasimov observed that there was no longer a clear distinction between war and peace.

Moreover, in modern warfare, increased emphasis is being placed on information and psychological warfare. Appropriately, it requires the use of non-military means of power, along with the armed forces, but has the potential to reduce the military power required (Gerasimov, 2016, p. 24; Bartles, 2016, pp. 30-31; Chekinov, Bogdanov, 2013, pp. 12, 16-17; Bērziņš, 2014, p. 5).

In the new generation of warfare, public institutions, media, religious organizations, cultural institutions, NGOs, public movements, criminals, and diplomats are all weapons of the aggressor state. All of these institutions aid in the information and psychological warfare that weakens the target state. *Obman* aids in this effort because these organizations use disinformation to help conceal military operations and the effort as a whole (Chekinov, Bogdanov, 2013, pp. 17, 18, 20; Bērziņš, 2014, p. 5).

RUSSIAN PSYCHOLOGICAL INFLUENCE AND *MASKIROVKA* AS A STATE OF MIND

From Clausewitz's (1832) fog-enhancing smokescreen of war, reinterpreted in particular by Dragomiroff (1889), to the informational smoke of social networks by *"troll factories"*, *maskirovka* corresponds to a codified set of processes designed to mislead, sow confusion, lead to fatigue, and, if possible, generate despair in enemies. It is thus an instrument that makes it possible to intervene in conflicts or in the balance of power that precedes them, while ensuring the stability of the state, which can therefore mobilize its forces without hesitation. This broad sense constitutes a form of *"doctrine of falsehood"* or relative truth in military, political or diplomatic terms. Of course, it includes all the metaphors of cunning and concealment, denial and lies, regardless of the evidence (Glantz, 1989; 1992). We thus resort to contents whose verification is complex and which go beyond mere omission or lying in order to rely on psychology: dispersion, illusion, logical paradoxes, cognitive biases... Moreover, it includes an ambition of targeted action to instil in people not only doubt, but also fear, dread and despair, regardless of the consequences for individuals and the social groups they compose.

Maskirovka is exercised simultaneously at all levels (Smith, 1966), from strategic to tactical or operational, and by all actors involved in the Russian state organization. Thus, it permeates all organs of the nation and has been applied in Soviet – now Russian – civil society. It is no longer just a military phenomenon, but also covers the fields of civil defence, internal security, and certain branches of industry, trade, agriculture or even artistic, cultural and digital production. The aim is to constantly deceive the real or potential adversary, relying on all the procedures of modifying

information processing, but also to determine the enemy to make mistakes (Karankevich, 2006); it is not only to disinform, but to misinform, overinform, sow doubts, saturate cognitive abilities, thus altering certainties.

Today's approaches mix both active and passive, physical, information and cyber actions. Furthermore, we can observe a form of similarity between Russian conceptions of *"psychological warfare"* (Ionov, 1994) and *"ideological struggle in peacetime"* with the *"information warfare"* waged by the West *"against its enemies in general and against Russia in particular"* (Prokhozhev, Turco, 1996). The action takes place, on the one hand, thanks to networks and the media, in science, education, public affairs management, culture, especially with the falsification of history (Minic, 2021) and, on the other hand , through targeted, precise and personalized attacks. The tools take on a new dimension with the emergence of social networks, news servers and public databanks, with *"trolls"* and cognitive cyber tools (digital *maskirovka*).

Maskirovka first targets Western culture and society as a whole by attempting to descend on individuals and influence or recode mass consciousness, for example to turn patriotism into collaborationism. The intent then descends to elites, community leaders, then employed as opinion leaders or agents of amplification. This procedure is similar to the *"key leader commitments"* or *"local leader actions"* of Western doctrine, without being constrained by moral boundaries. Ultimately, small groups can be reached, and individuals themselves can be subject to targeted actions through *"reflexive control"* (Thomas, 2016). Attacks that target individuals exploit their acquired or innate characteristics, weaknesses, and preferences to act on their behaviour as an agent, or their ability to command in context. In this way, the systems or institutions to which they contribute can be changed from the bottom up. It works at all levels and in both directions. It changes the coherence between leaders and the agents they command or the citizens they represent, between social entities and those who make them up.

Disinformation

Disinformation (with the literal meaning of *"erroneous information"*) is an example of a technique of influence widely used by the Soviet Union during the Cold War and taken up by current services, contributing to *maskirovka*. It consists in the systematic dissemination of false information in order to drown relevant information that could not be concealed (Schultz, Godson, 1984).

The first strategy is to hide information. Concealment is one of the main forms of disinformation. It involves procedures to reduce the ability to detect possible tell-tale signs of action or preparations for action: troops, equipment, strategic clues etc. Direct use of camouflage, hangars, canopies, camouflage cloths, paravanes in order to conceal stationing and lack of stationing, arming or placement of vehicles, ships, aircraft etc. The construction or storage of sensitive equipment can be carried out in this way, for example, in automobile factories, agricultural sheds or power stations.

The second strategy is imitation. It is based on the visible deployment of fake objects. The use of detachable or pneumatic models, intact parts of damaged equipment on wooden frames, drawings imitating reality or disruptive paintings (*"kamuflyazh"*), decoys and dummies, was frequently applied during the Second World War, and examples can also be found in recent conflicts, in Syria, in Crimea, and, more widely, in strategic seaports, through decoy bridges or the construction of factories or even unused airfields. Alongside passive imitation, simulation also has an active side. It consists of creating identifiable signs of activity to distract attention and increase the effectiveness of concealment. Examples are fictitious anti-aircraft or artillery emplacements, fake troop movements and convoys etc. (Smith, 1966).

The third strategy is to camouflage relevant information smothered in what it is not. The aim is to multiply global information by saturating the cybernetic communication channels of machines or the biological attention channels of individuals, thus sowing cognitive confusion.

The Global Approach has thus demonstrated remarkable abilities to combine military action, at all levels and in all areas, with non-military action. It can be seen in particular in the use of modern cyber tools and in the creation of real corps of specialists. But beyond this globality of actors, *maskirovka* is also a globalized phenomenon. It manipulates beliefs and perceptions by misinforming everyone. It takes on a global, chronic and generalized aspect for the entire social body. And it does not stop there, since it is accompanied by specific action on individuals: surveillance and possible discrediting of the bearers of information, discrediting those who analyse it, promotion of the bearers of fake news, the culture of *"useful idiots"* etc. The practice often resorts to associating public criticism or pejorative humour with threats.

This targeting is in itself a veritable method of applying the *"dossier culture"*, illustrated by the personalized discreditation of adversaries or globalized discreditation of groups represented by their leaders.

Demoralization

Demoralization (literally, the technique of *"demoralizing"*) is a procedure that has been used by Russian services to provoke a depressive syndrome or psychological distress and to propose an alternative strategy from which a person, group or state cannot evade or respond favourably, except at the risk of maintaining a pernicious state. For the victim, it does not matter what the solution is as long as the threat or psychological conflict ceases.

While this procedure is aimed at individuals, it is also aimed at the groups they make up, and therefore at the leaders of these groups, who are in a position to stop the suffering. The technique extended to adversary states is part of the arsenal of military art (*teoriya voyennogo iskusstva),* as *"the theory and practice of the preparation and conduct of the army and operations [...], as well as the use of «non-military» measures and indirect actions and other forms useful to the battle"* (Chekinov, Bogdanov, 2015, p. 24). In this context, psychological impact is considered a major strategic tool of influence, and demoralization is included in the art of warfare extended to any indirect means that contribute to success (Ib., p. 9). Demoralization can be considered as preparation of adversaries, groups and individuals, for submission and acceptance of alternatives favourable to Russia.

Like *disinformation*, *demoralization* concerns all state bodies and its institutions of public communication. In addition to the use of un-truths and all means of psychosocial influence, there are *"psychotronic"* and *"psychotropic"* means in psychological matters (Vorobyov, Kiselev, 2006). The former corresponds to actions and techniques involving direct human actions. This is the case of influencers, actors of relational actions, designers of targeted and adapted technical devices, such as computer programs or video productions etc. The other category of means concentrates indirect actions of neuropsychological or neurological induction, having a direct action on the brain and, consequently, on the morale. This is the case with drug use, certain psychotropic or narcotic drugs, electromagnetic emissions, control of delimited chemical, sound or light spaces, which cause transient or chronic mental health disorders [one example is the Havana syndrome (Verma et al., 2019)].

The proposed solution, although partial, is a favourable alternative for Russia. It can take the form of a defeat, a submission or a compromise which then opens up to blackmail. It is only with difficulty that the Western world understands that the authors can go beyond the ethical limits and observes, disarmed, that all the consequences for people's mental health do not enter into the equation of disastrous consequences: resignation, flight, drug use, alcoholism, melancholy, suicide, violence, induced personality disorders.

Digital Maskirovka

"Digital Maskirovka" is the application of the doctrine in the cyber world. The process consists of using troll factories to invade networks and Internet broadcasting systems and to identify flaws in systems in order to exploit weaknesses in technical or psychological usability. The digital space is considered as any flow of information and therefore a means of gaining an actual or potential strategic advantage. *Maskirovka* principles are widely applied in cyberspace (Bagge, 2019) with such ease, as manipulations are easy to implement, difficult to localize and, in the case of localization, always too late.

On the one hand, a saturation of information is practiced for disinformation and, on the other hand, the targeting of individuals or institutions allows the creation of individual *"dossiers"* based on historical website browsing and shopping habits, the intrusion of personal equipment, the corruption and mounting of files, real or invented, with posting on networks or under threat of judicial compromise. A plethora of non-geolocable or poorly localized front-ends are spread on the Internet by trolls, with fake or spoofed accounts, to influence either globally or in a targeted manner or to implement psychological influence operations.

False information sites or hijacked real sites, false testimonies, false theories or fragmented theories are thus put online, especially via social networks, after analysing internet usage habits. This is the case with lists of think tanks, trade unions or political parties, non-governmental associations, charities or advocacy organizations etc. The construction of fake, perfectly imitated websites, attempts to deceive users while manipulating them. One aspect to be mentioned is the intervention of trolls or specialized agents to anonymously or under false identity modify information in large databases on which content generation systems are based.

Finally, content crafted in an emotionally meaningful way is used to spread, encapsulated information in a viral fashion. The principle is to use a rationale for spontaneous (viral) dissemination of emotionally labelled messages (Berger, Milkman, 2012, pp. 192-205) to associate them with pieces of information as part of a reflexive control strategy. The source of information can be military, for example, Russian soldiers or mercenaries posting photos, videos or texts on social media, or bots that can transmit AI-generated synthetic images, movies or texts. The dynamics may be orchestrated by relays, but the spontaneity of *"useful idiots"* is sufficient for this widespread dissemination.

In all cases, there is a convergence of actions that modify structured thinking and those that manipulate emotions (Charquero-Ballester et al., 2023), such as

by using un-truths, half-truths or misleading information with a marked emotional dimension (Wunder, 2022, p. 7/1-7/5).

Maskirovka is primarily a state of mind. It is part of the spontaneous reasoning of the Russians and applies to all levels of the organization of the state, its diplomacy and its army, on the strategic, tactical or operational level (Smith, 1966).

This mindset is manifested in all branches or services of the Russian Armed Forces and, more broadly, in those of the state. As far as tactical units on the field of conflict are concerned, it also applies to all levels of the air force, air defence, border guards, intelligence and law and order services.

Thus, any *maskirovka* must be persistent, regardless of difficulty or questionable appearance, and even in the case of discovery or awareness by the enemy. The evolution must be slow, almost imperceptible, and lead the opponent or victim to incorrect estimations, false ideas, or to despair, submission, or abandonment. It must be plausible, i.e. the opponent or victim must be able to believe what is presented to him or maintain a rational doubt. *Maskirovka* must blend with the real or virtual environment, the physical or digital background and present plausible or ambiguous information. It should be varied, non-repetitive or as non-repetitive as possible and, if necessary, show visible differences. It is not intended to be spotted by statistical analysis or by the detection of common features that facilitate identification or anticipation by regularity or predictability. Lastly, there is a principle of continuity, at a geographical level, in the slow unfolding and temporality of actions, by installing a form of desperate chronicity situating any punctual action in a multidimensional background movement.

Therefore, the doctrine places every operation within a carefully defined and structured hierarchy of the *Maskirovka* state of mind in the Russian military thinking, or at least in the Russian military. Those who disregard its spirit are accomplices of the actual or potential enemy or, at the very least, bad citizens, and must be discredited, even punished.

HISTORICAL EVENTS MARKED BY *MASKIROVKA*

Historians have tracked the strategy since 1380, when the tsar Dmitry Donskoy and 50,000 Russian soldiers defeated 150,000 Mongol warriors of the Golden Horde at the Battle of Kulikovo. Donskoy's men achieved victory thanks to a surprise attack by a regiment of soldiers hidden in a nearby forest.

Maskirovka helped the Soviets achieve great victories several times during the Second World War, and since then it has been established as a general principle that has proven itself and is to be developed as a true specialty in defence

and security actions. Thus, while *maskirovka* is primarily an active support for military operations, it is no longer limited to the field of the military, but manifests itself both as a state of mind and as a permanent activity in a clearly applied orientation of hybrid warfare and a defensive state.

Battle of Kursk

The battle, which took place between 5 July and 23 August 1943, was the last offensive *blitzkrieg* action on the Eastern Front of the Second World War. *Maskirovka's* importance in Soviet military operations increased as the Soviet Army began offensive operations to retake Russian territory (Armstrong, 1988, p. 5). *Maskirovka* concealed the movement and grouping of Soviet formations for the counteroffensive. Specifically, the Battle of Kursk illustrated the effectiveness of Soviet *maskirovka*. The carefully planned and executed Soviet concealment effectively annihilated any chance the German army might have had to regain the offensive in Russia. In preparing for the battle, the Soviets used a series of *maskirovka* principles to ensure the secrecy of their preparations and intentions. The Kursk offensive primarily used *maskirovka* to conceal the movement, organization, and grouping of Soviet forces from German scout formations (Armstrong, 1988, pp. 5-6; Simms, 2003, p. 8).

The Soviet *maskirovka* during the Battle of Kursk was successful because the Soviets carefully considered the effect they were trying to achieve, planned the deception in detail, and used the available resources appropriately. Analysing the capabilities of the German Army informed the Soviets about what was necessary for a successful deception. The Soviet Army understood German intelligence collection, methods, systems, and capabilities. In planning the deception, the Soviets were able to ensure that the methods used were capable of avoiding German detection. The German Army was able to detect the units involved in the defence of Kursk, but was unable to identify the hidden defensive positions of the Steppe Front as to the true extent of the concentration of Soviet forces arranged in depth (Armstrong, 1988, pp. 26-27; Glantz and House, 1999, p. 74; Showalter, 2013, p. 66).

Later, throughout the war, Soviet military deception became increasingly sophisticated and effective through repeated practice. The Soviet Army learned, through repetition, the importance of centralized control and careful planning how to successfully use *maskirovka*. Practice proved that its execution required that false positions should be animated with at least ten percent of real troops and equipment (Armstrong, 1988, p. 16). The Soviets continued these lessons throughout the rest of the war to achieve surprise effects during other major operations.

The Cuban Missile Crisis

The Cuban Missile Crisis was a confrontation between the Soviet Union and the United States over Soviet nuclear missiles in Cuba. The crisis began on 14 October 1962 and lasted 38 days, until 20 November 1962. The crisis was seen as the moment when the Cold War came very close to becoming nuclear war and turning into the Third World War.

The attempts to deceive during the Cuban Missile Crisis are notable for both similarities and significant differences to the acts of deception during the Second World War. The Cuban Missile Crisis indicates a continued emphasis on the use of dissimulation and an increased emphasis on disinformation. In this way, the Soviets used *maskirovka* to conceal intentions similar to those during the Second World War. *Maskirovka* during the Cuban Missile Crisis differed from its application in the Second World War, with an increased emphasis on tactical, operational, and strategic disinformation.

In attempting to conceal the concentration of nuclear forces, the Soviet military used tactical concealment. It was demonstrated by the concealment of troops and equipment on ships docked in Cuba, by actions taken at the landing ports, and by concealing short- and medium-range ballistic missiles in Cuba. The success of Soviet concealment attempts was also quantified in the large number of Soviet military personnel moved to Cuba, largely undetected by the US military and the CIA[1] (Hansen, 2022, p. 54; McCone, 1992, pp. 19-20; Gribkov and Smith, 1994, pp. 27 28). However, the concealment attempts failed to hide the location of the surface-to-air missiles used to protect the ballistic missiles and their associated launch pads. In addition, the nuclear missiles, once in Cuba, had inadequate cover. This lack of cover led to the detection by the US military air reconnaissance service of the surface-to-air missiles and the launch pads they were defending. The large concentration of surface-to-air missiles contributed to the failure of the deception (Absher, 2009, pp. 29-31).

At the same time, the Cuban Missile Crisis displayed tactical, operational, and strategic *maskirovka* in its form of disinformation. Strategically, Soviet diplomats and political leaders made false statements that attempted to mislead US political leaders about the nature of Soviet intentions in Cuba. The clever naming of the military operation and the Soviet intelligence service's use of Cuban dissidents represented the operational use of disinformation in order to mislead. Ultimately,

[1] The Soviets managed to infiltrate over 40,000 soldiers and personnel involved in the concentration of ballistic missiles. In the months leading up to the crisis, the Central Intelligence Agency estimated that only 4,000–6,000 Soviet personnel were in Cuba.

the Soviet military's tactical disinformation of its own troops ensured the success of the non-disclosure of information about military plans by Russian forces.

Soviet *maskirovka* ultimately failed during the Missile Crisis for a number of reasons. First, the Soviets and Cubans failed to conceal the missile launch sites. Second, the Soviets and Cubans failed to adequately conceal the ballistic missiles. The final factor contributing to the failure of this *maskirovka* was suspicion. US government officials did not trust the Soviets and did not believe their narrative or messages. The lack of trust the US government displayed towards the Soviets made any statement suspect and open to scrutiny and verification (Alsop, Bartlett, 1988, p. 69).

Invasion of Czechoslovakia

The Invasion of Czechoslovakia, officially titled *Operation Danube*, was the occupation of the Czechoslovak Socialist Republic by armed forces from five Warsaw Pact member states – the Soviet Union, the Republic of Bulgaria, the Republic of Hungary, the GDR and the Republic of Poland – on the night of 20–21 August 1968. Approximately 250,000 soldiers occupied Czechoslovakia at the time. The invasion of Czechoslovakia ended the reforms initiated by Alexander Dubček in the Prague Spring.

The Soviet Union used a number of principles of *maskirovka* to achieve its objectives in Czechoslovakia. Disinformation fuelled existing popular fear, misdirected Czechoslovak military assets, and created a false presumption for the introduction of Soviet troops into the country. A simulated secret weapons depot provided evidence that made the entire Soviet disinformation campaign credible. Ultimately, the Soviets' use of the demonstration, in the form of military exercises, desensitized the Czechoslovak government and population to the true intentions of the Soviet forces. The combination of these factors allowed the Soviets to surprise both Czechoslovakia and Western governments with the invasion. Soviet intentions became clear once Czechoslovakia came under the full control of the Soviet Union.

Similar to Soviet attempts during the Cuban Missile Crisis, the Soviet intervention in Czechoslovakia demonstrated a continuing trend that coupled both military and diplomatic deception. At the tactical and operational levels, the Soviets used disinformation combined with simulations in an attempt to influence public opinion in Czechoslovakia. Military simulations in the form of manoeuvres and exercises postulated Soviet military forces for intervention. These manoeuvres and exercises further desensitized the Czechoslovak population and eliminated the Czechoslovak army as an obstacle to intervention. In addition, the manoeuvres strategically deceived Western governments about what was happening in Czechoslovakia.

Strategically, the Soviet political apparatus continued to use disinformation during their invasion in an attempt to conceal what was really happening in Czechoslovakia. Claims that the Soviets were invited into Czechoslovakia by disenfranchised political leaders misled Western nations about what was truly going on in Czechoslovakia and provided a credible basis for the Czechoslovak people.

Invasion of Ukraine

The invasion on 24 February 2022 constitutes an escalation of the Russo-Ukrainian War that began in 2014, following the annexation of Crimea by the Russian Federation in February-March 2014. The largest conflict in Europe since the Second World War has already caused hundreds of thousands of military victims and tens of thousands of Ukrainian civilian casualties.

The ongoing conflict in Ukraine highlights the increasing importance of the *obman* phenomenon in Russian military operations. The Russian invasion of Ukraine and the annexation of Crimea demonstrated the continuity between *maskirovka* and *obman* in the form of concealment, simulation, demonstrations, and disinformation. The conflict continues to expose how the Russian application of the *obman* principle has changed from its earlier versions in the Second World War, the Cuban Missile Crisis, and the intervention in Czechoslovakia. The invasion of Ukraine witnesses a shift in Russian deception. Plausible denial of the events that took place replaced the physical concealment of forces.

A significant difference between previous deception attempts and those in Ukraine is Russia's increased use of disinformation over other forms of deception. Disinformation is the cornerstone of the *obman* phenomenon in Ukraine. It is notable that most of the disinformation taking place in Ukraine is being executed throughout the Russian government. Russian political leaders, state media, trolls on government-controlled social media, and government agents are being used to spread false information and create false narratives around unfolding events. The scale of these actions dwarfs the diplomatic and intelligence efforts used during the Battle of Kursk, the missile crisis, and the invasion of Czechoslovakia.

Beyond the government's extensive use of disinformation, the Armed Forces of the Russian Federation have focused their efforts to deceive on simulations and demonstrations. The employment of the *"little green men"*, masked Russian soldiers in unmarked green uniforms, was a tactical and operational simulation of local partisan forces. Operationally, the demonstrations along the Ukrainian border of Russian military forces helped to focus Ukraine's attention away from Crimea.

The cover-up took place at a tactical level in order to infiltrate Russian soldiers into Ukraine. Beyond that, concealment helped with force protection and battlefield survival, but it did not play as large a role as it did during the Second World War or the Cuban Missile Crisis.

CONCLUSIONS

Maskirovka is no longer an old pre-Soviet practice that the communists developed as a theory of Russian military camouflage. It is a state of mind that today crosses military, political and diplomatic activities, in a culture of action of a Russia torn between distrust of external enemies and domination of those within. It has been enriched by disinformation, demoralization and techniques of manipulation and control, and has recently been amplified by the power of digital tools.

Maskirovka is conceived in the field of psychological warfare, in accordance with the knowledge and guidelines of the great Russian psychological tradition. Few works are translated, the first ones, especially on behaviourism, were rewritten by Westerners, at the same time as Russian universities and psychology centres were self-enclaving. Apart from the conquest of space, which is a particular area of collaboration with the West, little is known about recent Russian psychology, neither fundamental nor applied to individuals or small groups and collectives, nor about systemic social experiments.

The analysts' writings reveal several features, however. Thus, unlike Western military work, which is focused on social and political sciences, Russian practice combines all dimensions of human action and action on the people. It attaches great importance to biology, neuroscience, psychology, but also physics and radiation. The method is global, associating actions from the top down, at the social level for the effects on the individual, and from the bottom up, focusing on the individual for the effects on human groups, all of which are in a continuous loop and regarded as complementary.

Another feature is the insensitivity of the actors to the fate of the targets, although it is often fatal. Morality has nothing to do with the case here, except for Russia's interests. The action is also often triggered, conducted, then abandoned, when it becomes effective and has achieved its goal. Moral disarmament, repeated surprise and continuous astonishment of democratic countries represent some of the weaknesses constantly exploited. Each time, the unimaginable astounds the victims who are always surprised. The culture of slowness, of potential power, is another striking characteristic of *maskirovka*. It is made to last by being inscribed in the consciousness of an eternity of Russia.

BIBLIOGRAPHY:

1. Absher, K.M. (2009). *Mind-Sets and Missiles: A First-Hand Account of the Cuban Missile Crisis*. Carlisle, PA: Strategic Studies Institute, http://www.strategicstudiesinstitute.army.mil/pdffiles /pub935.pdf, retrieved on 9 August 2024.
2. Alsop, S., Bartlett, Ch. (1988). *"Eyeball to Eyeball"*. In *The Cuban Missile Crisis*, ed. Robert A. Divine. New York, NY: Markus Weiner Publishing.
3. Armstrong, R.N. (1988). *Soviet Operational Deception: The Red Cloak*. Fort Leavenworth KS: Combat Studies Institute.
4. Bartles, Ch. K. (2016). *"Getting Gerasimov Right".* In *Military Review* (January-February), pp. 30-38.
5. Berger, J., Milkman, K.L. (2012). *"What Makes Online Content Viral?".* In *Journal of Marketing Research*, vol. 49, no. 2, pp. 192-205.
6. Bērziņš, J. (2014). *Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy*. Riga, Latvia: National Defense Academy of Latvia Center for Security and Strategic Research.
7. Charquero-Ballester, M., Walter, J.G., Sletten-Rybner, A., Nissen, I.A., Enevoldsen, K.C.&Bechmann, A. (2023). *"Emotional landscapes of misinformation spread"*. Helsinki: NORdic observatory for digital media and information DISorders (NORDIS) reports.
8. Cekinov, S.G., Bogdanov, S.A. (2011). *"Strategy of Indirect Approach: Its Impact on Modern Warfare"*. *Voennaia Mâsli*, vol. 20, no. 3. pp. 9-15.
9. Cekinov, S.G., Bogdanov, S.A. (2015). *"The Development of Modern Military Art from the Vantage Point of Systemology"*. *Voennaia Mâsli,* vol. 24, no. 11, pp. 22-28.
10. Cekinov, S.G., Bogdanov, S.A. (2013). *"The Nature and Content of a New-Generation War". Voennaia Mâsli*, vol. 10, no. 4, pp. 12-23, http://www.eastviewpress.com/Files/MT_FROM%20THE%20CURRENT%20ISSUE_No.4_2013.pdf, retrieved on 10 October 2024.
11. Clausewitz (von), C. (1832). *Vom Kriege*. Berlin: F. Dümmler. Traduction Naville, D. (1998). *De la guerre*. Paris: Éditions de Minuit.
12. Dragomiroff, M. (1889). *Principes essentiels pour la conduite de la guerre – Clausewitz commenté.* Paris: L. Baudoin et Cie.
13. Gherasimov, V. (2016). *"The Value of Science is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations".* In *Military Review* (January-February), pp. 23-29.
14. Glantz, D. (1989). *Soviet Military Deception in the Second World War*. London: Routledge.
15. Glantz, D. (1992). *The Military Strategy of the Soviet Union: A History*. London: F. Cass.
16. Glantz, D.M., House, J.M. (1999). *The Battle of Kursk*. Lawrence, KS: University Press of Kansas.
17. Gribkov, A.I., Smith, W.Y. (1994). *Operation Anadyr: U.S. and Soviet Generals Recount the Cuban Missile Crisis*. Chicago: Edition q.
18. Hutchinson, W. (2004). *"The Influence of Maskirovka on Contemporary Western Deception Theory".* In Jones A. (Ed.) *Proceedings of the 3rd European Conference on Information Warfare and Security.* Reading (United Kingdom): Academic Conferences Ltd, pp. 165-174.

19. Hansen, J.H. (2002). *"Soviet Deception in the Cuban Missile Crisis". Studies in Intelligence,* 46, no. 1, pp. 49-58.
20. Ionov, M.D. (1994). *"Psikhologiceskie aspektî upravleniia protivnikom v antagonisticeskih konfliktah (refleksivnoe upravlenie)". Prikladnaia ergonomika*, no. 1, pp. 44-45.
21. Karankevici, V.I. (2006). *"Kak naucitsa obmanâvat protivnika". Voennaia Mâsl*, vol. 15, no. 9.
22. Lindley-French, J. (5 April 2018). *"Skripal: Countering (Again) Strategic Maskirovka"*, https://lindleyfrench.blogspot.com/search?q=maskirovka, retrieved on 10 October 2024.
23. McCone, J.A. (1992). *CIA Documents on the Cuban Missile Crisis*. Edited by Mary S. McAuliffe, pp. 19-20. Washington DC: Central Intelligence Agency.
24. Minic, D. (2021). *La guerre informationnelle psychologique dans la pensée militaire russe et ses applications en Ukraine et en Syrie*. Annuaire français de relations internationales. Paris: Éditions Panthéon-Assas, vol. 22, pp. 523-533.
25. Prohojev, A.A., Turko, N.I. (17 February 1996). *"Osnovi informaţionnoi voinî".* Proceedings of the first conference on Systems Analysis on the Threshold of the 21st Century: Theory and Practice, Moscow (Russia), pp. 250-258.
26. Schultz, R.H, Godson, R. (1984). *Dezinformatsia: Active Measures in Soviet Strategy.* New-York: Pergamon.
27. Simms, B.R. (2003). *"Analysis of the Battle of Kursk". Armor: Mounted Maneuver Journal* (March-April), pp. 7-12.
28. Smith, C.L. (1966). *"Soviet Maskirovka".* In *Air Power Journal*, vol. 2, no. 1, pp. 28-39.
29. Showalter, D.E. (2013). *Armor and Blood: The Battle of Kursk, the Turning Point of World War II.* New York, NY: Random House.
30. Thomas, T. (2016). *"Russia's 21st century information war: working to undermine and destabilize populations".* In *Defence Strategic Communications,* Riga: NATO Strategic Communications Centre of Excellence, vol. 1, pp. 16-25.
31. Thomas, T.L. (2011). *Recasting the Red Star*. Fort Leavenworth, KS: Foreign Military Studies Office.
32. Verma, R., Swanson, R.L., Parker, D., Ould Ismail, A.A., Shinohara, R.T.& Alappatt, J.A., Doshi, J., Davatzikos, C., Gallaway, M., Duda, D., Chen, H.I., Kim, J.J., Gur, R.C., Wolf, R.L., Grady, M.S., Hampton, S., Diaz-Arrastia, R., Smith, D.H. (2019). *"Neuroimaging Findings in US Government Personnel with Possible Exposure to Directional Phenomena in Havana, Cuba"*. In *Journal of the American Medical Association*, vol. 322, series 322, no. 4, pp. 336-347.
33. Vorobiov, I.N., Kiselev, V.A. (2006). *"Strateggia neprâmâh deistvii v novom oblike". Voennaia Mâsli,* vol. 16, no. 9.
34. Wunder, M. (2022). *"Narratives overwhelme the world"*. In B. Claverie, B. Prébot, N. Buchler, F. du Cluzel (eds.). *Cognitive Warfare: The Future of Cognitive Dominance*. NATO Collaboration Support Office, pp. 7/1-7/5.

WORST-CASE SCENARIOS FOR A TURBULENT WORLD – MODELLING HOW FAR AND HOW COSTLY DEFENCE AND SECURITY COULD GO –

Professor Iulian CHIFU, PhD
Center for Conflict Prevention and Early Warning, Bucharest, Romania
DOI: 10.55535/RMT.2024.4.13

The turbulent world we are living in now prompts planners and prospective studies specialists to address the requests of worst-case scenarios and catastrophe scenarios with low probability and high impact, to draft the level of costs of tackling such threats in the short, mid and long-term. It is also a part of the debate about costs and consequence-oriented finances of the security and defence, and resumes the level of ambition and capacity of a state to fulfil one of its basic responsibilities. A change of leadership in the US presidential race and in the administration, perspectives of NATO as a common defence organisation that ensures today's defence and security guarantees in Europe, extreme right forces in key governments of democratic European member countries, pro-Russian forces with veto rights in governmental policies, debate about nuclear umbrella possible changes, all constitute scenarios that someone would not wish to analyse. But no responsible government or leader of a country, at least from the Eastern Flank, could avoid foresee and prepare for even the tiniest possibility that such a scenario happens in 6-12 months, 3-5 years, 10-15 years. Our paper researches a number of worst-case scenarios, impact, consequences and costs in order to warn about the need for prospective studies and preventive anticipated actions for a credible deterrence and a suitable defence. Our methodology is in the prospective studies field, in the niche of the worst-case scenarios and catastrophe scenarios.

Keywords: scenarios; tipping points; relative certainties; critical uncertainties; cost oriented/ consequence-oriented security planning;

INTRODUCTION

The theory of worst-case scenarios, as that of the catastrophe or extraordinary events, gives us the opportunity to reflect on the perspectives of the long term, high intensity, full-scale war of aggression of Russia in Ukraine (Chifu-13, 2024). Discussing that low probability, high impact crisis and outcomes are usually ruled out from the analysis or marginalised, if not, of course, overrated and used for inducing panic and stress to a targeted population, when political needs require it.

That is why we need clarity even in this field and a balanced approach to this type of scenarios that need to be considered due to their high impact and the conditions and context that made them appear, in spite of low probability. This is prompted and accentuated in times of turbulence. Moreover, because of the lack of preparedness, paralysis inside the societies, even the most resilient ones, *ad hoc* interventions of decision-makers, that could even accentuate these extreme crises to heights difficult to manage, are quite possible.

We are applying our Romanian Methodology of prospective studies (Chifu-7, 2022), in order to extract the worst-case scenarios and then, applying the theory of worst-case scenarios, we extract and present only these credible and possible scenarios, that we consider to be critical for any planning, even though the public communication of such scenarios should be subject to a restricted public, with adequate warnings and disclaimers for an exact understanding of the needed warnings facing such evolutions.

PROSPECTIVE STUDIES. THE ROMANIAN METHODOLOGY

We introduced the Romanian Methodology of prospective studies in 2013[1], using the technique of the Dutch intelligence services presented in a *Global Future Forum* conference (Chifu-1, 2013; Chifu-2, 2014), and filled the gaps with solid theoretical steps that offered us this methodology applied in a number of studies. The essence is to split the work into a brainstorming phase of indicators of influence to the assessed evolution, related to both internal and external factors. The method

[1] PLATO is an abbreviation for *PLAusible TOmorrows* – a plausible tomorrow, plausible future scenarios. It is originally a scenario-building tool – used for the construction of scenarios by the Dutch services AIVD, proposed and presented to a number of experts in prospective studies at a demonstration. The authors of the presentation are Marja Schinkel, analyst, and David Blum, analyst.

is linked to global security and international relations and offers a huge number of indicators to be scrutinised afterwards by specialised experts that would eliminate indicators that do not make sense or add, according to the ideas that could emerge in the debate of the brainstorming phase, new indicators[2].

The second phase, after clarifying the indicators, is to refine the pool on indicators such that they are creating a system non-contradictory and complete, as synthetic as possible. We will get finally 4-5-6 indicators with 2-3-5 values possible to model, with the lowest error of the model. Moreover, the full spectrum of scenarios will be divided in continuity and discontinuity ones, prompted by tipping points (Chifu, Bălăşoiu, 2018; Chifu, Getmanchuk, Nantoi, 2015; Chifu-3, 2015; Chifu-2).

For each case, we are realising at the expert level two pools of elements: critical uncertainties (Rhydderch, 2017) about the evolution of the event analyded and relative certainties (Monroe, Beruvides, Tercero Gómez, 2020, p. 51) of the same evolution. The result is used in the first case to verify the system of critical indicators selected is complete, in the second case, we are challenging each relative certainty with *black swan* scenarios. This should challenge the relative certainty obtained with propositions that all experts would consider valid. Here is the source of our worst-case scenarios, when the impact of such changes could lead to catastrophes according to Rene Thom definition (Thom, 1986)[3].

WORST-CASE, CATASTROPHIC CASE, „*BLACK SWAN*" EVENTS. THE THEORY OF THE MOST IMPROBABLE, BUT POSSIBLE SCENARIOS

In 2012, Nigel Walpole launched the debate on thinking about the unthinkable (Walpole, 2012) based on distinct cultural and ideological horizons that are creating unexpected and unpredictable actions by the opposite side. The concept evolved in the unthinkable in the context of the opponent's nuclear actions (Kahn, 1985) or the prospect of a dictator of the world, whom all peoples will acclaim and support, accepting him (White, 1992) and to the economic dimension of *thinking the unthinkable* (Cockett, 1995). The limits and difficulties of leadership in predicting and avoiding unexpected developments (Gowing, Langdon, 2015) and Nik Gowing in the book published in 2018 (Gowing, Langdon, 2018), consecrated the approach. Nine were the reasons for difficulties and unthinkable:

1. overwhelming of decision-makers with intense and multiple pressures;

[2] Iulian Chifu, *Studii prospective și metodologii alternative... op.cit.*

[3] "*Modèles mathématiques de la Morphogenese*" (1974), ed. Christian Bourgeois, Paris; "*La thèorie des catastrophes*" (22 December 1976), Paris: Le Monde.

2. institutional compliance;
3. deliberate blindness;
4. group-think – compliant group thinking;
5. risk aversion;
6. fear of career-limiting movements;
7. reactionary thinking systems;
8. denial;
9. dissonances and cognitive overload (Ib.).

Donald Rumsfeld on 12 February 2002, in a briefing at the Pentagon (DoD, 2002), introduces the reference to known knowns, known unknowns and unknown unknowns – unknown knowns was missing. The concept has been previously approached: the known and unknown space was divided between the self and others, a fact resumed by Johan Galtung when he proposed the Cain and Abel model (Chifu, Lupu, 2016; Ramsbotham, Woodhouse, Miall, 2011, p. 9; Galtung, 1969, p. 168; Galtung, 2000, p. 1), but the term *unknown unknown* was used by NASA[4] and is commonly used in project management and strategic planning (Courtney, Kirkland, Viguerie, 1997).

David C. Logan reviewed the triad of terms in the context of general scientific research, biology, in this particular case (Logan, 2009, pp. 712-714). Thus, scientific research itself can be placed in the form of the action of transforming known unknowns into known knowns. A final answer on how we identify the unknown unknowns is difficult to pronounce. If we knew how to reach these elements, in practice, we would have the immediate transformation of the unknown unknowns into known unknowns. It is an open topic.

The most important author for managing the risks of extreme events is Nassim Taleb, with his book, in 2007, on the highly improbable (Taleb, 2007). He had the proof that one single observation can invalidate a general statement derived from millennia of confirmatory sightings. Organisations failed to deal with the demands of extreme events which, by definition, are crises (Chifu-4, 2019; Chifu, Ramberg, 2007; Chifu, Ramberg, 2008), but a class with outcomes that have very high consequences (often exceeding the perceived worst-case scenario) but also have a low probability of occurrence (Fischbacher-Smith, 2010, pp. 1-8). Their unique nature makes them important for research and theory. The most current examples

[4] See the hearings on 24-25 June 1981 that took place in the Commission for Science and Technology of the House of Representatives of the US Congress, at https://books.google.be/books?id=dRMrAAAAMAAJ&pg=PA73&dq=%22unknown+unknowns%22&hl=en&sa=X&ved=0ahUKEwjhnraJ-7XmAhVGi1wKHUi0Bl0Q6AEIKTAA#v=onepage&q=%22unknown%20unknowns%22&f=false retrieved on 22 August 2024.

are in aviation, space (Shuttle Challenger), but also geo-physical phenomena such as natural hazards.

The precautionary approach is often advocated within the academic literature (Calman, Smith, 2001, pp. 185-204). The likelihood of an accident required considerable investment and a loss of revenue, and the lack of historical evidence often led organisations and individuals to argue that the probability of the hazard being realised was so low that building early warning or other mitigation strategies becomes un-economic. A key element here was that this *"denial"* was a function of the lack of *a priori* evidence that was available to decision-makers (Dilnot, 2008, pp. 36-39).

Taleb and others suggest that instead of trying to anticipate low-probability, high-impact events, we should reduce our vulnerability to them. Risk management, we believe, should be about lessening the impact of what we don't understand – not an attempt to develop sophisticated techniques that perpetuate our illusions of being able to understand and predict the social and economic environment (Taleb, Goldstein, Spitznagel, 2009, pp. 78-81). This means being *"crisis prepared"* or *"resilient"* (Chifu, pp. 10-21; Chifu-8, 2022, pp. 3-10; Chifu-9, 2022, pp. 5-14; Chifu-10, 2022, pp. 3-10). It should be linked especially to recognising the limits of knowledge, but it is very difficult to know what we do not know.

At the same time, another tendency is that when managers are faced with events about which they do not know anything, the process is broken, panic can emerge, lack of solutions are pushing to bad ad-hoc decisions and then there is the potential to generate *"points of inflection"* which can escalate the problem further (Handy, 1994; Handy, 1995). In some cases, these approaches could lead from an escalating crisis to extreme events and catastrophes, with the secondary crisis emerging as consequences of the very decisions that would be expected to curve the impact or the original crisis. Therefore, the study of extreme events, worst-case scenarios, or catastrophe requires a strong relation and interface with research and professional counselling in crisis decision-making.

COST AND CONSEQUENCES. EFFECTIVENESS IN RISK MANAGEMENT AND EXTREME EVENTS

Another important debate is related to reactions in times of crisis and preparedness when cost-oriented programs are applied linked to resources. The models to consider would be terrorism versus global heating (Sunstein, 2009). The idea is that resources are scarce and difficult to allocate to all threats, risks and vulnerabilities, so it must be a sequence and prioritisation. And in financing security, the first most important approach is a cost-oriented one, where budgets

are allocated according to the probability of the events to occur. But the critics have introduced a new approach, consequence-oriented, where a share of the budget, let us say 20%, are allocated to threats with low probability by high impact, including extreme events and worst-case scenarios (Chifu-6).

In the case of terrorism, another part of the game comes from perceptions. It is highly dangerous to ignore such a threat very visible, with a huge emotional and perceptive reaction from the population and it is easier to do so, from this point of view, with the global heating (Chifu, Simons, 2023). In another example, very debated nowadays, we are considering cheap drones and expensive air-defense missiles: should we intercept them? Considering the cost-oriented approach to security, some would say that it does not worth firing a missile (Viscusi, Aldi, 2003; Heinzerling, 2004). Consequence-oriented experts (Posner, 2006; Posner, 2004) would rather look at the outcomes and argue that you cannot afford let even a cheap drone destroy an ammunition storage that worth billions and otherwise supports the war effort, or that an aircraft blown up worth some billion dollars as well, so the value of a possible target and intangible costs of an impact should be equally considered in those cases.

We also have the One Percent Doctrine or the Precautionary Principle, which is specifically designed for situations in which we cannot know that harm will occur. If it goes below 1% it is not worth considering it. It is different when the probability goes above or if the costs of the impact is higher (Suskind, 2006). Even a small risk of catastrophic or irreversible harm is enough to require a serious response. But, at the same time, if the world devotes resources to climate change, for instance, on those grounds, perhaps it will not be able to use those resources to combat more serious problems like imminent terrorist attack. This is the cost-consequence dilemma.

Vice President Dick Cheney set out The One Percent Doctrine: *"We have to deal with this new type of threat in a way we haven't yet defined... With a low-probability, high-impact event like this... If there's a one percent chance that Pakistani scientists are helping al Qaeda build or develop a nuclear weapon, we have to treat it as a certainty in terms of our response"*. Vice President Cheney urged that governments identify and attempt to prevent, the worst-case scenario (Weber, 2006).

People and decision-making reactions to risks as well as to worst-case scenarios, come from two different angles. The first is intuitive, based on personal experience that leads to fearing the outcome of crisis that have been already occur and have harmed us. It is emotional rather than objective basis. By contrast, the other group tend to believe that we are talking about an unlikely event that is not worth

resources and attention. It is what happens with the institutions as well: paying both too much or, on the contrary, too little concern with low-probability risks. An important task is to find the right balance of exceptional events or worst-case scenarios so that errors are not influencing behaviour when assessing the worst-case scenario relevance (Ib.).

The same in the case of rational choices and bias. The absence of a type of event make decision makers and the public feel far more secure because of the *"unavailability bias"*. The terrorist threat could be neglected or treated with less interest and resources in countries that did not face currently or from a long time such events. The opposite is also true, with the *"availability bias"* after a terrorist attack, when that context would indicate and press to allocate resources exactly for this kind of possible event (Akerlof, Dickens, in Akerlof, 1984). For sure, here perception should be also considered and the sense of safety to the population. Therefore, it is important exploring risk perceptions, when preparing our responses to worst-case scenarios.

The Precautionary Principle could be amended in two ways an replacing the 1% rule: one, a Catastrophic Harm Precautionary Principle, that approaches the fact that when catastrophic risks become factual reality, they could come with more serious consequences than planners and analysts originally foresee, because of *"social amplification"*. When worst-case scenarios have catastrophic consequences, it makes sense allocating resources to anticipate or cope with consequences or avoiding the risk *per se* (Posner, 2006). The same with the Irreversible Harm Precautionary Principle, which would introduce a special attention when consequences of an extraordinary event or crisis leads to irreversible situation and post-conflict reconstruction is not going to remake things the way there were.

Risk evaluation and insurances offer another angle of approach to worst-case and to consequence-oriented allocation of resources for extreme or catastrophic low probability events. In this case, cost-oriented processes are linked to loss and destruction of industrial security interests like material assets and humans beings, in some cases to symbolic and immaterial/intangibles (Chifu-11, 2024). A method to assess risk and security is linked to the effectiveness of integrated protection system – facility operations, safety, emergency, and security systems; and qualitative prioritization scheme to determine the level of consequences relative to cost and subsequent risk (Udell, Rogers, 1998).

Human Security is rather cost-oriented (Acharya, 2001, pp. 442-460). Self-sustaining security can be seen both as a requirement and as the most urgent objective with consequence and cost oriented approach (Chivvis, Davis, 2011) alike.

Theory and empirical work as well as statistical-empirical analysis show that the *"cost theory"* of counterinsurgency leads to a consequence-oriented approach because of the need of increasing the costs of cooperating with an insurgency as the surest means to victory (Austin, 2006), but that can happen only with immense reputational costs.

SQUARING THE CIRCLE: WAYS TO PREPARE DETERRENCE AND RESILIENCE IN AN UNCERTAIN WORLD

Now the worst-cases that are subject to Catastrophic Harm Precautionary Principle or Irreversible Harm Precautionary Principle should be subject to the attention of the decision-maker and should have a suitable allocation of resources. We have done the sequence of prospective studies related to *black swan* scenarios and selected those low probability-high impact scenarios that fit into the Catastrophic Harm Precautionary Principle. So, we succeed in finding the following seven scenarios, linked to seven relative certainties:

- US will remain involved in the world affairs and in adaptation of new rules.
- Dictatorship is not an option acceptable for democratic countries.
- NATO will remain and function with both of its legs of the transatlantic/US will not withdraw from the Alliance.
- Extreme right will not rule and divide the EU countries.
- Pro-Russian forces will not veto democratic government decisions if they enter the government in a democratic country.
- US will maintain its nuclear umbrella on the European allies.
- Russia will not use a nuclear weapon.

They lead to those *black swan* scenarios:

S1. Isolationism and retreat of the US from the world through a change of leadership at the White House, in the current or next US presidential race.

S2. China and BRICS/revisionist authoritarian countries will propose alternative authoritarian regimes, embraced by the people, and this would lead to the change of the rules-based order.

S3. NATO will lose the US – being paralysed in its decisions or dissolved, or will lose the transatlantic link. Gloomy perspectives of NATO as a common defence organisation that ensures today's guarantees in Europe.

S4. Extreme right forces entering in key governments of democratic European member countries are negotiating rights that create blockages of European policies through democratic decisions.

S5. Pro-Russian forces will have veto rights in governmental and European policies in the EU.

S6. Debate about nuclear umbrella possible changes: US withdraws from its WWII/NATO commitments (demanding money from the protected countries, asking for political and/or market advantages etc.)

S7. The use of a tactical nuclear weapon by Russia in Ukraine or in some NATO/EU country in the Eastern Flank.

What we could see is that all those scenarios come from *black swan* events, contested, with low probability of becoming facts, but with high impact if events occur. Moreover, in each case, we have either catastrophic or irreversible outcomes or huge impact. All the conditions for considering the worst-case are met, according to our precedent definitions. In that case, all should become scenarios to be considered and require planning for solutions in the event such alternative futures happen.

Debate could be raised by some of the scenarios, where the previous data could lead to a discontinuity and not a *black swan* scenario:

- S1 where we do have a president that aims at a kind of isolationism, but in his previous term, he maintained his and US position inside the euro-Atlantic community;
- S3, when retreat from the Alliance has been used in the public communications of a possible US president. But the condition of the investments in defence and security has changed dramatically and member countries are meeting, at a large respect, the Defence Pledge, with a minimum 2% of the GDP allocated for defence and at least 20% for new equipment.
- S7, where intelligence disclosed has proven that the use of a Russian nuclear weapon was discussed in 2023, during the counteractions of Ukraine, but fell short of support. Some other arguments could be discussed if there is not a discontinuity scenario rather than a *black swan* one. In all those cases, arguments sit today and in the foreseeable future in the *black swan* side of highly improbable evolutions (Chifu-12, 2024).

The solution for such a crisis, extreme event or worst-case scenario is building both resilience and a serious defence and deterrence. And it includes:

- Attractiveness of the military activity.
- A new social contract with those employed in the Army and Security positions.
- Capabilities acquired in the short term, with high technological components, and the possibility to adapt in an ongoing use in war times.
- Doctrines and strategies learnt from the first 21st century war in Europe, Russia's war of aggression in Ukraine.

- Military and defence industry, transformed at the level of a vigilance stage (an intermediary between peace and war, considering that a bloody war is evolving in a country neighbour to the EU and NATO and that direct threats from Russia are coming in a public and overt way against the West.

In conclusion, all those scenarios should be the object of the allocation of needed resources and to planning for worst-case scenarios, in a consequence-oriented approach to security in every responsible country.

BIBLIOGRAPHY:

1. Acharya, A. (2001). *Human Security: East versus West*. In *International Journal*, vol. 56, nr. 3 (summer), pp. 442-460, Sage Publications.
2. Akerlof, G.A., Dickens, W. (1984). *The Economic Consequences of Cognitive Dissonance,* in Ackerlof, G.A., *An Economic Theorist's Book of Tales*, pp. 123, 124-128. Cambridge: Cambridge University Press.
3. Austin, L. (2006). *On "Other War": Lessons from Five Decades of RAND Counterinsurgency Research*. California: Santa Monica, RAND Corporation, http://www.rand.org/pubs/monographs/MG482.html, retrieved on 12 May 2024.
4. Calman, K., Smith. D. (2001). *Works in Theory But Not in Practice? Some Notes on the Precautionary Principle*. Public Administration 79 (1), pp. 185-204.
5. Chifu, I.-1 (2013). *Analiză prospectivă. Experiența internațională și o abordare românească*, in *Revista Română de Studii de Intelligence,* nr. 10, December, ISSN 2067-3353.
6. Chifu, I.-2 (2014). *Prospectives on Ukraine Crisis. Scenarios for a Mid-Long Term Evolution*. București: Editura ISPRI, ISBN 978-606-8656-01-4.
7. Chifu, I.-3 (9 October 2015). *Prospective Analysis of Ukrainian Crisis: Scenarios for Mid-Long Term Evolution*. Ukraine: Odessa, *Ukraine Analytica*, nr. 1, ISSN 2518-7481.
8. Chifu, I.-4 (2019). *Decizia în criză*. București: Editura RAO, ISBN 978-606-006-349-0.
9. Chifu, I.-5 (2021). *Reziliență strategică: de la stabilitate și prevenție la acțiune pro-activă și adaptabilitate dinamică/Strategic Resilience: from Stability and Prevention to Pro-Active Action and Dynamic Adaptability*, in *Gândirea militară românească,* nr. 1/*Romanian Military Thinking*, nr. 1.
10. Chifu, I.-6 (2022). *Amenințări și conflicte în secolul 21.* București: Editura RAO, ISBN 978-606-006-818-1.
11. Chifu, I.-7 (2022). *Studii prospective și metodologii alternative. Eșafodajul de securitate în secolul 21*. București: Editura RAO.
12. Chifu, I.-8 (2022). *Lecțiile conflictului din Ucraina și perspectivele rezilienței societale*. In *Infosfera,* nr. 2.
13. Chifu, I.-9 (2022). *Reziliență contemporană: competitivitatea națiunilor, capabilitatea statelor și securitatea societală*. In *Infosfera,* nr. 3.
14. Chifu, I.-10 (2022). *Constructul și tematica rezilienței stratificate*. In *Infosfera,* nr. 4.
15. Chifu, I.-11 (2024). *Resilience, Societal Security and the Intangibles of War. Ukraine's Lessons Learnt*. In *Romanian Military Thinking*, nr. 1, https://en-gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20reviste/RMT/2024/1/CHIFU.pdf., retrieved on 22 August 2024.

16. Chifu, I.-12 (2024). *Retorică nucleară rusă între război informațional și credibilitatea unei acțiuni necugetate*. In *Infosfera*, nr. 2, https://www.mapn.ro/publicatii_militare/arhiva_infosfera/documente/2024/2_2024.pdf., retrieved on 22 August 2024.
17. Chifu, I.-13 (2024). *Russian War of Aggression and Perspectives of the Wider Black Sea Region. Future Studies and Alternative Scenarios*. International Congress *"Changing Strategic Security Landscape in the Black Sea and the Balkans: Challenges and Opportunities"*, AREL University. Türkiye: Istanbul, https://usam.arel.edu.tr/changing-strategic-security-landscape-in-the-black-sea-and-the-balkans-challenges-and-opportunities/, retrieved on 22 July 2024.
18. Chifu, I., Bălășoiu, N. (2018). *Prospective Studies of the Wider Black Sea Region. Scenarios for its Future in Times of High International Turbulence*, Editura ISPRI, București, ISBN 978-606-8656-62-5.
19. Chifu, I., Lupu, L. (2016). *Analiză de conflict*. București: Editura RAO, ISBN: 9786067760262.
20. Chifu, I., Nantoi, O., Getmanchuk, A. (2015). *Prospective on Ukraine Crisis. A Trilateral Approach*. București: Editura ISPRI, ISBN 978-606-8656-21-2.
21. Chifu, I., Ramberg. B. (2007). *Crisis Management in Transitional Societies*. CRISMART SNDC. Sweden: Stockholm, ISBN 978-91-85401-64-2, ISBN 1650-3856.
22. Chifu, I., Ramberg, B. (2008). *Managementul crizelor în societăţile în tranziţie, Cazul României*. Bucureşti: Editura RAO, ISBN 978-973-103-687-8.
23. Chifu, I., Simons, G. (2023). *Rethinking Warfare in the 21st Century. The Influence and Effects of the Politics, Information and Communication Mix*. Cambridge University Press, ISBN: 9781009355247.
24. Chivvis, C.S., Davis, P.K. (2011). *Establishing Security,* in Paul K. Davis, *Dilemmas of Intervention. Social Science for Stabilization and Reconstruction*, Rand Co, retrieved on 22 July 2024.
25. Cockett, R. (1995). *Thinking the Unthinkable: Think-tanks and the Economic Counter-revolution 1931-1983*. Harper Collins, ISBN 978-0006375869.
26. Courtney, H., Kirkland, J., Viguerie, P. (1997). *Managing Uncertainty, Strategy under Uncertainty*. Harvard Business Review, November-December, https://hbr.org/1997/11/strategy-under-uncertainty, retrieved on 22 July 2024.
27. Dilnot, C. (8 December 2008). *The Triumph of Greed*. New Statesman, pp. 36-39.
28. DoD News Briefing – Secretary Rumsfeld and Gen. Myers, Presenter: Secretary of Defense Donald H. Rumsfeld, 12 February 2002, https://archive.defense.gov/Transcripts/Transcript.aspx?TranscriptID=2636, retrieved on 22 July 2024.
29. Fischbacher-Smith, D. (2010). *Beyond the Worst-Case Scenario: "Managing" the Risks of Extreme Events*, in Risk Management, nr. 12, pp. 1-8. DOI: 10.1057/rm.2009.17, retrieved on 22 July 2024.
30. Galtung, J. (1969). *Violence, Peace, and Peace Research*, in *Journal of Peace Research*, vol. 6, nr. 3.
31. Galtung, J. (2000). *Conflict Theory and Practice: A Perspective*, in *Conflict Transformation by Peaceful Means (Transcend Method)*. United Nations Disaster Management Training Programme, United Nations.
32. Gowing, N., Langdon, C. (2015). *Thinking the Unthinkable, A New Imperative for Leadership in the Digital Age*, 21st century Statesmanship Global Leaders Programme, https://www.slideshare.net/nudripakke/pdf-download-thinking-the-unthinkable-a-new-imperative-for-leadership-in-the-digital-age-pdf-free, retrieved on 16 December 2019.
33. Gowing, N., Langdon, C. (2018). *Thinking the Unthinkable: A New Imperative for Leadership in the Digital Age.* John Catt Educational Ltd., ISBN 978-1911382744.
34. Handy, C. (1994). *The Empty Raincoat: Making Sense of the Future*. London: Hutchinson.
35. Handy, C. (1995). *The Age of Unreason. New Thinking for a New World*. London: Random House.
36. Heinzerling, L. (2004). *Priceless: On Knowing the Price of Everything and the Value of Nothing*. New York: New Press.
37. Kahn, H. (1985). *Thinking the Unthinkable in the 1980's*. Touchstone, ISBN 978-0671604493.
38. *La thèorie des catastrophes* (22 December 1976). Paris. In *Le Monde*.
39. Logan, D.C. (2009). *Known Knowns, Known Unknowns, Unknown Unknowns and the Propagation of Scientific Enquiry*. In Journal of Experimental Botany, vol. 60, nr. 3, pp. 712-714, https://doi.org/10.1093/jxb/erp043, retrieved on 22 December 2019.
40. Monroe, T., Beruvides, M.G., Tercero- Gómez, V. (2020). *Quantifying Risk Perception: The Entropy Decision Risk Model Utility (EDRM-U)*, December, Systems 8(4):51.
41. Posner, E.A. (2006). *New Foundations for Cost-Benefit Analysis*. Cambridge: Harvard University Press.
42. Posner, R. (2004). *Catastrophe: Risk and Response*. New York: Oxford University Press.
43. Ramsbotham, O., Woodhouse, T., Miall, H. (2011). *Contemporary Conflict Resolution. The Prevention, Management and Transformation of Deadly Conflicts*, 3rd edition. Cambridge: Polity Press.
44. Rhydderch, A. (June 2017). *Scenarios Building: the 2x2 Matrix Technique*, in Futuribles.
45. Suskind, R. (2006). *The One Percent Doctrine 61-62*. New York: Simon & Schuster.
46. Sunstein C.R. (2009), *Worst-Case Scenarios*. London: Harvard University Press, Cambridge Massachusetts.
47. Taleb, N.N. (2007). *The Black Swan. The Impact of the Highly Improbable*. London: Penguin Books.
48. Taleb, N.N., Goldstein, D.G., Spitznagel, M.W. (2009). *The Six Mistakes Executives Make in Risk Management*. In Harvard Business Review, nr. 87 (10), pp. 78-81.
49. Thom, R. (1986). *Teoria Catastrofelor*. București: Editura Didactică și Pedagogică; *Modèles mathématiques de la Morphogenese* (1974). Paris: Christian Bourgois.
50. Udell C.J., Rogers, B.H. (1998). *Risk Evaluation: A Cost-Oriented Approach*. Fluor Daniel Hanford.
51. Viscusi, W.K., Aldy, J.E. (2003). *The Value of a Statistical Life: A Critical Review of Market Evidence throughout the World*, in *Journal of Risk and Uncertainty*, vol. 27(1).
52. Walpole, N.J.R. (2012). *Thinking the Unthinkable: The Lives of Royal Air Force and East German Fast-Jet Pilots in the Cold War*. Astonbridge Publishing, ISBN 9780953793327.
53. Weber, E.U. (2006). *Experience-Based and Description-Based Perceptions of Long-Term Risk: Why Global Warming Does Not Scare Us (Yet)*, in Climatic Change, vol. 77, 103, Springer Nature Link.
54. White, J.W. (1992). *Thinking the Unthinkable*. World Publishing, ISBN 978-0850095678.

ADAPTATION OF NATO TO THE NEW REALITIES FROM ALLIED EASTERN AND SOUTHERN FLANKS

Vasile-Dumitru RAȚIU, PhD Student
National School of Political and Administrative Studies, Bucharest, Romania
DOI: 10.55535/RMT.2024.4.14

NATO has had to constantly adapt to the new challenges that emerge on the global stage. In order to succeed, the Alliance has adapted each time its involvement has been requested. In this regard, NATO has well overcome the problem of fighting terrorism, improving cyber security and the effort required to remain in solidarity with Ukraine to date. On the eastern flank, NATO is strengthening its defences by increasing the number of troops and weapon systems available and rethinking defence plans to deal with possible aggression from the Russian Federation. On the southern flank, the North Atlantic Alliance wants a consolidation of states in North Africa and the Middle East that have been divided by civil wars and better management of illegal migration. All the new challenges that have arisen and may arise require a thorough preparation of NATO members for an increasingly unstable future. The purpose of this article is to present how NATO is adapting to the challenges coming from the eastern and southern flanks. The hypothesis I am starting from is that NATO's adaptation to the new realities on the two flanks represents a challenge for the organization. The research method used in this article is the case study.

Keywords: NATO; Eastern flank; Southern flank; Russian Federation; Ukraine;

INTRODUCTION

The challenges for NATO, from its beginnings (April 1949) to the present, caused by geopolitical changes, have been multiple and complex. NATO had to reinvent itself after several unforeseen changes, such as: the end of the Cold War (when the main adversaries – the Warsaw Pact and the USSR – disappeared), the challenge brought by the rise of international terrorism and the emergence of new powers in Asia.

The 21st century is characterized by the trend of continuous change. At the political, economic, social and military level, the world is changing, as a result of the emergence of the phenomenon of resistance to globalization. Every international actor wants to remain competitive and be able to provide a clear vision on how to manage emerging issues.

The world, based on economic cooperation and open societies, could not exist if every power imposed trade taxes and, through military power, imposed spheres of influence. In this century, in addition to the classic challenges, new challenges have emerged that the North Atlantic Alliance must face.

New challenges have arisen on NATO's eastern flank due to the modernization of the Russian military arsenal and the desire of the Russian Federation to regain its old spheres of influence. Another challenge for NATO is given by the maintenance of a tense situation in the area of the South Caucasus and the Black Sea, where there are frozen conflicts that can be reactivated at any time. The most recent case was the resumption of the conflict between Armenia, supported by the Russian Federation, and Azerbaijan, militarily supported by Türkiye, since September 2023.

Following the annexation of Crimea in 2014, the conflict between the Russian Federation and Ukraine resumed on 24 February 2022. According to Moscow officials, this *"special operation"* was aimed at removing the neo-Nazi leadership from Kyiv, demilitarizing Ukraine and supporting Russian brothers in the two self-proclaimed independent republics of Donetsk and Luhansk. The prolongation of this conflict led to the need for some allied states, neighbouring Ukraine, to support this state more and more, in order not to be defeated.

After the terrorist attacks of 11 September 2001, the USA began an all-out war against terrorism, involving other allied states and even NATO. The UN issued a resolution that represented the legal framework for states' fight against terrorism. Non-state actors such as the terrorist organizations Hamas and Hezbollah, along with Yemen's Houthi rebels, have become a source of security threat due to their ability to operate regionally. These organizations, financed by Iran, endanger the security of the State of Israel and the entire security environment in the region. Houthi rebels are a danger to shipping in the Red Sea and Gulf of Aden.

In the 21st century, the use of computers and satellites in communication has increased the speed of data and information transmission. This is beneficial both economically and militarily. If data transmission networks are overloaded, they freeze and stop working. The first NATO member state to be cyberattacked was Estonia in 2007. Since then, NATO and the EU have secured their cyberspaces. Thus, an Allied Centre of Excellence for Cyber Defence Cooperation (CCDCOE) was created in Tallinn.

Moreover, this century is one of continuous change; *"In the 21st century, social ties are transnational, mutual dependencies are global. Covid-19 amply demonstrated this, as did the far-reaching consequences of Russian aggression against Ukraine. In Central Europe, related debates on EU enlargement, economic development challenges, as well as political, social and cultural ones are intertwined"* (Pries, 2023, p. 1).

The purpose of this article is to present how NATO is adapting to the challenges coming from the eastern and southern flanks. The three main objectives of the research are: to present the existing situation in NATO's eastern flank by analysing the challenges from this flank, to analyse the existing situation in NATO's southern flank by highlighting the challenges in the Middle East and North Africa (MENA), and to detail the role played by NATO in combating terrorism. The hypothesis I am starting from is that NATO's adaptation to the new realities on the two flanks represents a challenge for NATO. The research method used in this article is the case study. In order to find out how NATO is preparing to respond to the multiple challenges to which it is obliged to respond, we used the following sources of documentation: official NATO and UN websites and documents (www.nato.int, www.un.org, *Washington Summit Declaration*, *United Nations Global Counter-Terrorism Strategy*), specialist articles and media sites.

CHALLENGES FOR NATO ON THE EASTERN FLANK

NATO and the EU are trying to help certain states in Eastern Europe, such as Ukraine, the Republic of Moldova and Georgia. NATO has partnerships with these states in various fields of activity in order to increase the capacity of the armed forces. The EU, through financial and logistical support, wants to bring the eastern states closer together and prepare them for future EU accession. These efforts were made difficult by the presence of separatist entities within these states: *"Not surprisingly, the frozen conflicts in the former Soviet space are located in the strategically important region of the Black Sea, on the territory of sovereign states such as Azerbaijan (Nagorno-Karabakh)[1], Georgia (Abkhazia and South Ossetia), the Republic of Moldova (Transnistria) and, more recently, Ukraine (the so-called ‹people's republics› of Donetsk and Lugansk)"* (New Strategy Center, 2016, p. 3). Crimea was occupied in 2014 amid great instability in Ukraine following the 2013 Euromaidan.

In order to better understand the Eastern region of Europe, especially the former states of the USSR that emerged after the collapse of the communist colossus, the issue of frozen conflicts on their territory must be highlighted. All these conflicts are related to the Russian Federation (Ib.). *"Moscow steps in to impose ceasefires or other temporary arrangements, halting hostilities for a time but leaving the root causes untouched. In some cases, this entails the continuation of the Russian military presence in the form of ‹peacekeeping troops›, in order to secure additional leverage for long-term geopolitical advantages. Moscow's interest in generating and maintaining such foci of latent tension is to control the whole (sovereign states or areas of strategic interest) by establishing control over a part (the conflict zone)"* (Ib., p. 4).

The maintenance of influential figures, who are directly controlled from Moscow, has led over time to the effective control of those regions by the Russian Federation. In this context, Russia's power in the area remained intact for a long time.

The failure to resolve these old conflicts has led to a dilemma for some EU and NATO member states regarding the progress of the eastern states towards their full integration into these two organizations. The unresolved conflict in Ukraine has halted the rise and smooth trajectory towards NATO and the EU.

[1] After the 2023 conflict, as of 1 January 2024, the Nagorno-Karabakh region (Karabakh of Mountain) definitively re-entered under the authority of Azerbaijan, therefore we can no longer speak of a *"frozen conflict"* in Azerbaijan.

It all culminated in the desire of the Russian Federation to change the leadership in Kyiv and annex parts of Ukraine. More than two years have passed since the invasion on 24 February 2022. The war has been at a stalemate for a long time, both sides having problems with troop morale and insufficient stock of weapons and ammunition. After the armed forces of Ukraine entered the territory of the Russian Federation and occupied an area of more than 1,000 square kilometres in the Kursk region, the situation of the war remained uncertain. Kyiv claims that this moment represents a position of strength from which peace negotiations with Moscow could begin.

Another challenge for the North Atlantic Alliance that is considered to be overcome concerns the migrant crisis on the border between Poland and Belarus. These actions on the eastern border of NATO and the EU are considered part of a hybrid war that wanted to destabilize the allied states on the eastern flank.

Researcher Crăișor-Constantin Ioniță believes that the world is moving towards a division into two competing blocs: *"Since the beginning of this war on the Eastern European border, considered by politicians and military leaders as the biggest major regional conventional conflict since the end of the Second World War, the international community has been divided and grouped into supporters of each belligerent, only a few countries remaining neutral. Therefore, we can say that, ‹de facto›, we already have a world divided into two opposing blocs – the Western democracies (NATO, EU, G7) that support Ukraine against the authoritarian regimes (BRICS, most of the G20) close to Russia"* (Ioniță, 2024, p. 10).

Professor Maria Mälksoo appreciates that, on the eastern flank, NATO is increasing its military forces again. During the Cold War, the Americans had about 300,000 troops in Western Europe, which decreased greatly after 1990, only after the aggression of the Russian Federation and the annexation of Crimea, in 2014, the American troops beginning to increase, reaching in 2022 about 100,000 (Mälksoo, 2024, p. 538). *"NATO's new Strategic Concept, adopted at the alliance's 2022 Madrid summit, marks its coming full circle, as the alliance's eastern flank is currently undergoing a remilitarization effort more reminiscent of the Cold War era than the alliance's post-Cold War leitmotiv of avoiding drawing a new dividing line in Europe"* (Ib.).

Regarding the Black Sea, analyst Ondrej Ditrych (2024) believes that there are *"four possible security scenarios"* for the next decade:

1. *Lake interregnum.* The current evolution is maintained, in which case the Russian Federation and Ukraine continue fighting in the Black Sea, and *"all forms*

of security, including maritime navigation and infrastructure" (Ditrych, 2024, pp. 2-3) are hampered. There is a very high risk of untoward incidents and significant damage to the commercial maritime sector.

2. *Russian lake.* The most dangerous scenario in Ditrych's view. In this scenario, the Russian Federation will control the Black Sea. The scenario assumes the involvement of the Russian Federation *"on multiple fronts – through a successful offensive in southern Ukraine, skilful manipulation of domestic politics in Moldova and Georgia, and potentially pressuring Türkiye to reopen the Straits"* (Ib., p. 3). This would mean that the Russian Federation would own most of the Black Sea coast and control a significant portion of maritime activity (Ib.).

3. *European lake.* It would be the most optimistic scenario due to the cooperation of every Black Sea littoral state, with the exception of the Russian Federation, with the EU. *"Ukraine regains control of Crimea which ceases to be Russia's strategic bastion. NATO and the EU manage to field denial and intelligence, surveillance and reconnaissance capabilities to secure Black Sea navigation and critical infrastructure (including platforms and undersea cables)"* (Ib.).

4. *Lake glacialis.* It is a scenario in which a new Cold War would take place between the Russian Federation and NATO, which would divide the region politically and economically. Depending on the outcome of the current Russian-Ukrainian war, the Black Sea security zone could be included in a larger model of European security architecture (Ib.).

Among all these scenarios, the most convenient for Romania would be the *European lake* scenario, through which both security and commercial interests would be guaranteed.

The Russian-Ukrainian conflict highlighted the need for NATO to increase weapons production and the adaptation of the defence industry to new requirements (Olay, 2024). General Christopher G. Cavoli, Commander Allied Forces Europe (SACEUR), argues that: *"It is extremely important that we get this right (...) because I believe that the industrial production of defence items is a critical part of our integrated deterrence"* (Ib.). As a result, it is necessary to create new production capabilities in all allied states.

To strengthen the eastern flank, a state-of-the-art radar from Italy was brought to Romania. *"Radar will mainly be used in military applications to provide comprehensive situational awareness and improve the operational capabilities of various platforms, including military ships and submarines"* (EurActiv, 2024).

In addition to reinforcements with troops and weaponry from the allied eastern flank, better collaboration with NATO partners in the region is needed on the southern flank.

CHALLENGES FOR NATO ON THE SOUTHERN FLANK

The Russian Federation threatens not only the eastern flank but also the southern flank by creating military bases in Syria and Libya. Through these bases, the Kremlin gets involved in the internal conflicts in these states, supplying weapons to one of the parties. Through this military involvement, the Russian Federation hopes to control these states and gain a bridge to the states of Central Africa and the rest of the Middle East.

In order to have an advantageous position on the southern flank, Moscow began to diversify its positions in the Mediterranean. The best positions are those in Syria, especially the one in the port of Tartous, which is an important distribution centre of armaments for the rest of the military bases. *"In addition to gaining control over natural resources (oil and gas) and the Mediterranean port of Tartous, Russia gained a prominent position to bargain with the US in other countries such as Ukraine and Libya"* (Beaujouan, 2024, p. 8).

Another port located in Libya, Tobruk, is used by Moscow to arm the group led by Marshal Khalifa Haftar, who controls eastern Libya. The same port is a bridge to the states of Central Africa, where Russian paramilitary groups, such as Wagner, operate.

To deal with these changes in the Middle East and North Africa (MENA) and to remove any threat, NATO proposes a deepening of relations with most states in the region. Dalgaard-Nielsen (2022) argues that NATO will have a very difficult task in stabilizing this region. *"Meanwhile, the instability emanating from NATO's southern flank, and the threats from terrorism, organized crime, and irregular mass migration, remain. Political, ethnic, and religious tensions, lack of good governance, a worsening climate crisis, food shortages, proliferation of weapons, and emerging disruptive technologies, will continue to add fuel to conflicts in this region. It is highly doubtful whether current alliance efforts in the South, including NATO's mission in Iraq (NTM-I), will be sufficient to leave any lasting positive impact on the stability of the region"* (Dalgaard-Nielsen, 2022, p. 169).

The anniversary NATO summit in Washington in 2024 reaffirmed the unity among the allies and the desire to continue on the same path to maintain the current world order, based on rules and norms. On the 75th anniversary of the founding

of the North Atlantic Alliance, the member states proposed the strengthening of NATO and the need for continuity was emphasized. NATO grew to include 32 members, the last two of which – Finland and Sweden – made the move to the alliance after the Russian-instigated war began. At this summit, which took place between 9-11 July this year, NATO presented in the final statement how the relations between the organization and the states in the southern neighbourhood should evolve: *"NATO's southern neighbourhood provides opportunities for cooperation on issues of mutual interest. Through our partnerships we aim to foster greater security and stability in the Middle East and Africa, contributing to peace and prosperity in the region. In Vilnius, we launched a comprehensive reflection on threats, challenges, and opportunities in the South"* (NATO, 10 July 2024).

Also at this summit, the North Atlantic Alliance adopted an action plan for NATO's southern flank. The plan will be updated according to the needs of the Alliance: *"Today we have adopted an action plan for a stronger, more strategic and result-oriented approach toward our southern neighbourhood, which will be regularly updated. We have invited the Secretary General to designate a Special Representative for the southern neighbourhood who will serve as NATO's focal point for the region and will coordinate NATO's efforts"* (Ib.).

The collaboration with the states of the southern part of the Alliance will continue and be strengthened by creating new liaison centres that will improve relations between NATO and these states: *"We will reinforce our dialogue, outreach, visibility, and our existing instruments for cooperation, such as the Defence Capacity Building Initiative, the Hub for the South and the NATO-ICI Regional Centre in Kuwait. Together with the Hashemite Kingdom of Jordan we have agreed to open a NATO Liaison Office in Amman. Building on the success of NATO Mission Iraq (NMI) and based on the request of the Iraqi authorities, we have broadened the scope of our support to the Iraqi Security Institutions and will continue our engagement through NMI"* (NATO, 10 July 2024). In addition, cooperation between NATO and partners on the southern flank is necessary to stop the development and spread of terrorism.

TERRORISM IN THE 21ST CENTURY

The terrorist attacks in the United States that occurred on 11 September 2001, caused by Al-Qaeda, changed the US position on terrorism. International terrorism has been and continues to be a threat to international peace and security. This phenomenon is described by NATO as: *"The unlawful use or threatened use of force or violence, instilling fear and terror, against individuals or property*

in an attempt to coerce or intimidate governments or societies, or to gain control over a population, to achieve political, religious or ideological objectives" (NATO, 19 August 2016).

The attacks of 11 September 2001, like those that followed in Europe, changed the perspective on security in democratic states around the world. Terrorism is one of the most complex phenomena of the 21st century that has become a reality with great global implications, difficult to prevent and manage. At the same time, another important moment that affected the whole world was the US decision by which the US government initiated a global military campaign against international terrorism, involving NATO in this war.

Non-state actors such as the terrorist organizations Islamic State (ISIS) and Al- Qaeda have become a source of security threat due to their ability to operate regionally and globally and within the state.

The causes that lead to terrorism are: international conflicts, failed state, occupation of a territory, as well as lack of economic development of the state. These cases highlighted the link between terrorism, radicalism and violent extremism, which must be stopped.

The complex issue of terrorism has also been addressed by the UN. In the discussions of the Sixth (Legal) Commission – 71st session, the issue of terrorism was extended to the financing of these groups. *"Furthermore, some delegations expressed concern at the nexus between transnational organized crime and terrorism, while other delegations expressed the view that the issues should be understood and addressed separately. In this regard, many delegations stressed the need to address the question of the paying of ransom money, underlying that it constitutes one of the key sources of income for terrorist groups"* (UN, 11 November 2021).

Therefore, it is necessary to understand the factors that influence terrorism in order to be able to prevent people from joining various terrorist groups. The management of this type of threats within international organizations has led to the creation of counter-terrorism strategies (NATO, 5 December 2023). *"NATO's work on counter-terrorism focuses on improving awareness of the threat, developing capabilities to prepare and respond, and enhancing engagement with partner countries and other international actors"* (Ib.).

The UN proposes a global strategy against terrorism, which is a method of regional and international stimulation to combat terrorism. The UN strategy commits countries to combat terrorism at local, regional and international levels.

In this struggle, countries must respect human rights. They must provide citizens with peace, tranquillity and freedom.

The UN strategy is composed of 4 pillars:

1. "Measures to address the conditions conducive to the spread of terrorism.

2. Measures to prevent and combat terrorism.

3. Measures to build States' capacity to prevent and combat terrorism and to strengthen the role of the United Nations system in that regard.

4. Measures to ensure respect for human rights for all and the rule of law as the fundamental basis of the fight against terrorism" (UN, *United Nations Global Counter-Terrorism Strategy*).

The issue of international terrorism is an integral part of the challenges to which NATO must adapt. NATO member states, at the initiative of the US, took the necessary measures to combat international terrorism, by modifying security strategies and increasing resilience.

CONCLUSIONS

NATO meets the multiple challenges on its eastern and southern flanks by continuously strengthening and adapting and providing a balanced political-military response. The new changes on the eastern flank forced NATO to take new measures to balance the report of forces in the area. For NATO, the Russian Federation represents the main threat in the short and medium term. The Russian Federation is involved in the destabilization of candidate states for accession. The expansion of NATO in the eastern flank, through the future accession of Ukraine, Georgia and the Republic of Moldova, represents a challenge for the entire alliance, but also a *"red line"* for the Kremlin.

On the southern flank there are several crises and conflicts that may affect the MENA region and, by extension, NATO member states. The conflict between Hamas, Hezbollah and Israel, with the involvement of Iran, has led to extreme tension in the Middle East. As a result, despite NATO's best efforts, the MENA region will be difficult to stabilize, given the conflict in Gaza and Lebanon, Iran's threats to Israel, Türkiye's stance on Israel's military actions, and frequent military coups in the region Sahel and West Africa.

The outbreak of the conflict in Gaza was based on a terrorist action, in which armed and well-trained individuals attacked civilians. The Russian Federation is actively involved in Syria and Libya by creating military facilities that allow

it to control the region. It also has logistics and military facilities in two major ports in Syria (Tartous) and Libya (Tobruk).

All the new challenges that have arisen and may diversify require a thorough preparation of NATO member states for an increasingly unstable future and a permanent adaptation of the North Atlantic Alliance to the requirements of the regional and global security environment.

BIBLIOGRAPHY:

1. Beaujouan, J. (2024). *Power Peace: The Resolution of the Syrian Conflict in a Post-Liberal Era of Peacemaking*. In *Journal of Intervention and State building*, pp. 1-20, https://doi.org/10.1080/17502977.2024.2371713, retrieved on 22 June 2024.
2. Dalgaard-Nielsen, A. (2022). *Tackling Strategic Simultaneity: What NATO Could Do to Adapt to the New Multitude of Threats*. In *Scandinavian Journal of Military Studies*, 5(1), pp. 165-176, https://doi. org/10.31374/sjms.143, retrieved on 12 May 2024.
3. Ditrych, O. (18 July 2024). *Four Swans of the Black Sea: Security scenarios for a contested region*. *European Union Institute for Security Studies*, 1-4, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_2024-13_BlackSea_web.pdf, retrieved on 12 August 2024.
4. EurActiv. (2024). *Radar NATO de ultimă generație, relocat din Italia în România*, https://www.euractiv.ro/politic-intern/radar-nato-de-ultima-generatie-relocat-din-italia-in-romania-68306, retrieved on 2 September 2024.
5. Ioniță, C.-C. (2024). *Entering the Third Year of the Russia – Ukraine War: What Might Happen in the Near Future*. In *Strategic Impact*, 90(1), pp. 9-22, https://cssas.unap.ro/en/pdf_periodicals/si90.pdf#page=9, retrieved on 12 August 2024.
6. Mälksoo, M. (2024). *NATO's new front: deterrence moves eastward*. In *International Affairs*, 100(2), pp. 531-547, https://doi.org/10.1093/ia/iiae008, retrieved on 22 May 2024.
7. NATO (5 December 2023). *Countering Terrorism*, https://www.nato.int/cps/en/natohq/topics_77646.htm., retrieved on 4 August 2024.
8. NATO (19 August 2016). *NATO's Military Concept for Defence against Terrorism*, https://www.nato.int/cps/en/natohq/topics_69482.htm, retrieved on 4 August 2024.
9. NATO (10 July 2024). *Washington Summit Declaration*, https://www.nato.int/cps/en/natohq/official_texts_227678.htm, retrieved on 2 August 2024.
10. New Strategy Center (2016). *De ce contează Marea Neagră*, https://newstrategycenter.ro/wp-content/uploads/2016/04/Policy_paper_-_De_ce_conteaza _Marea_Neagra_-_NSC_-_iunie_2016-1.pdf, retrieved on 2 August 2024.
11. Olay, M. (9 August 2024). *Ukraine War Illustrates Need for Robust Defense Industry, Eucom Commander Says*. *U.S. Department of Defense*, https://www.defense.gov/News/News-Stories/Article/Article/3868506/ukraine-war-illustrates-need-for-robust-defense-industry-eucom-commander-says/, retrieved on 11 August 2024.

12. Pries, L. (2023). *From Economic Remittances to Societal Transmittances Experiences from the European Union*. In *Contemporary Southeastern Europe*, 10(1), pp. 1-20, https://contemporarysee.org/allfiles/documents/file-127-from-economic-remittances-to-societal-transmittances-experiences-from-the-european-union.pdf, retrieved on 22 August 2024.
13. UN (11 November 2021). *Measures to eliminate international terrorism*, https://www.un.org/en/ga/sixth/71/int_terrorism.shtml, retrieved on 4 August 2024.
14. UN. *United Nations Global Counter-Terrorism Strategy*, https://www.un.org/counterterrorism/un-global-counter-terrorism-strategy, retrieved on 8 August 2024.

APPLICATION OF NATO MODELS FOR BUILDING INFORMATION INFRASTRUCTURE IN CRISIS SITUATIONS

Violeta VASILEVA, PhD
Future Innovation Labs, Sofia, Bulgaria
Associate Professor Veselina ALEKSANDROVA GAGAMOVA, PhD
Rakovski National Defence College, Sofia, Bulgaria
DOI: 10.55535/RMT.2024.4.15

The effective functioning of the national security system during disasters, accidents and other crisis situations related to cyber security and cyber defence requires the realization of opportunities for inter-institutional interaction of all elements of the system. This paper presents certain opportunities as part of the methodology to apply NATO models to develop the system design of information infrastructure with capabilities to achieve the required levels of operational interoperability to respond to cyber threats to national security. For the architectural configuration, the NATO Technical Reference Model (NTRM) is applied and the NATO Common Operating Environment Component Model (NCOECM) is used for defining the information infrastructure components of the system design. By implementing the proposed methodology, a model of architectural configuration of an information infrastructure of a Security Operations Centre component has been developed – the Security Information Event Management (SIEM) Server. A specification of the technical and software configuration of the SIEM server is developed.

Keywords: NATO models; methodology; cybersecurity and cyber-defence; system design; interoperability and resilience;

INTRODUCTION

Informational infrastructure comprises a unity of its components, the relations among them, the principles and rules that govern their design and development. Security Information Event Management (SIEM) server as a component of cybersecurity informational systems should be architecturally configured by implementing the proposed NATO models. For that purpose, a model of an information infrastructure component (SIEM server) has been developed with a specification of its technical and software configurations by using the two main NATO references models: 1. NATO Technical Reference Model (NTRM) and 2. NATO Common Operating Environment Component Model (NCOEM) [Allied Data Publication 34 (ADatP-34)].

Architectural development requires modelling, which helps us understand the connection between the requirements, on the one hand, and the architectural concept, on the other hand. The requirements must be presented in a chart format according to NATO C3 Technical Architecture Implementation Handbook [ISSC NATO Open Systems Working Group, AC/322(Sc/5)N268, 2002]. The NC3TA-IHB identifies in Annex A the templates that need to be filled out by project managers and architects, but does not provide a methodology how to do this. It is up to the project managers and architects to choose appropriate methodologies that fit their needs. There is a need for a methodology to fill out the NC3TA templates from Annex A. A proposal for such methodology is presented by the authors. As an example of the application of such a methodology, the paper presents the development of the architectural configuration of SIEM server.

MODELS FOR ARCHITECTURAL CONFIGURATION OF THE COMPONENTS OF THE INFORMATION INFRASTRUCTURE OF SYSTEMS IN CRISES MANAGEMENT ENVIRONMENT

For achieving the resilience of Information Systems in Cyber Conflict Environment it is necessary that the development of cybersecurity systems for organizations should be interoperable. Therefore, the application of NATO models would assist the development of organizations' cybersecurity systems.

One of the main models of system compatibility is the NATO Technical Reference Model (NTRM). It is a model for describing the information environment,

defining applications data and information infrastructure components data. It also defines the service areas (capabilities that are grouped by function) as well as their interfaces. The structure of the Technical Reference Model considers the separation of data from applications as well as applications from software configuration. The model is designed to separate applications and the external environment from the platform. It allows for the application compatibility and the independence from external devices (i.e., Keybords, Mouse, Webcam, USB Drive, External Hard Drive, Joystick, Game Controller etc.). For this purpose, the model defines the Application Program Interfaces (APIs) and the External Environment Interfaces (EEI).

The NTRM model includes five layers – three categories of objects (entities) and two interfaces, as follows:

- Application Software Entity;
- Application Program Interface/API;
- Application Platform Entity;
- External Environment Interface/EEI;
- External Environment Entity.

The application software consists of user and supporting software applications (software) or, as it is generally popular, user and application software.

Application Programming Interfaces (APIs) are applications that implement the connection between the service and the platform, i.e., applications between the application software and the application environment.

The application environment platform contains a system of services that physically materialize the information processes, i.e., system services and physical environment services (data exchange).

External Environment Interfaces (EEIs) provide the user with access to data and applications. Moreover, they provide connections between the application and the external environment. The concept of Internal Interfaces complements the description of APIs and EEIs.

The External Environment Entity includes external services that interact with those of the physical environment of the application software. These services are classified into the general categories of user services (mouse, display), information exchange services, and communication services (Local Area Network/LAN, Wide Area Network/WAN).

According to NTRM, the Application Platform Entity includes the following 12 Application Platform Service Areas (Allied Data Publication 34/ADatP-34):

- User Interface Services.

- Data Management Services.
- Data Interchange Services. These services provide support for the interchange of data between applications on the same or on heterogeneous platforms.
- Graphics Services. These services provide functions required for creating and manipulating graphics.
- Communication Services. These services provide distributed applications support for data access and applications interoperability in heterogeneous or homogeneous networked environments.
- Operating System Services.
- Internationalisation Services. Within the context of the NTRM, internationalisation provides a set of characteristics and data representation services.
- System Management Services.
- Security Services.
- Distributed Computing Services. These services provide specialised support for applications that may be physically or logically dispersed among computer systems in a network.
- Software Engineering Services.

Common Command and Control (C2) Applications Services. These services provide the ability to view data (i.e., share) in a common way across the network. Common C2 Applications Services promote interoperability among diverse functional mission area domains.

DEFINING THE ORGANIZATION OF THE COMPONENTS OF THE INFORMATION INFRASTRUCTURE OF THE CYBERSECURITY SYSTEM

For the effective functioning of the Computer Security Incident Response Team (CSIRT), it is necessary to provide the following components of the information infrastructure of the cybersecurity system in organizations:

- technological equipment with the relevant sensors for monitoring the communication and information infrastructure;
- intrusion detection and prevention systems – IDS/IPS/IDPS; (Intrusion Detection and Prevention Systems/IDPS is used to integrate IDS and IPS technologies);

- systems for processing and analysis of computer incidents – Security Information Event Management (SIEM) to support the actions of the team in reading a large number of registered events from cyber defence sensors;
- video surveillance systems, Next Generation Firewalls;
- trained and highly qualified personnel in the field of cyber defence;
- software for cyber forensics;
- a web server with cyber awareness information service.

The services to be provided by the SOC[1] can be divided into three main categories:

- response services (reactive services) provided in response to incidents – the main purpose of these services is to limit the damage caused by incidents;
- preventive incident response services (proactive services) – these services include detecting and reducing the possibility of a potential incident or event related to the security of the information system or network being protected;
- security improvement services – these services help to improve the quality of internal security. They are provided by experts in the field so that effective joint activities can be carried out within the organization so as to indirectly prevent the occurrence of incidents.

It is extremely important to react quickly and effectively when security breaches occur. One of the advantages of the incident response capability is that it maintains a systematic incident response (i.e., successive incident handling) so that appropriate action can be taken. Incident response helps staff minimize the loss or theft of information and disruption of services caused by accidents.

Security Information Event Management System

The use of the Security Information Event Management (SIEM) system for processing and analysing computer incidents is proposed as an incident response system. SIEM solutions provide a comprehensive view of the network in real time and help teams be more active in combating security threats (*"What Is SIEM?"*, n.d.). The advantage of SIEM solutions is that they combine security event management (SEM), which performs data analysis for events and real-time log files to ensure event correlation, incident response threat monitoring, with Security Information Management (SIM), which retrieves and analyses audit data and generates a report.

[1] Computer Security Incident Response Team (CSIRT) or Security Operations Centre (SOC), CERT/CC (Computer Emergency Response Team/Coordination Center, IRT (Incident Response Team), CIRT (Computer Incident Response Team), SERT (Security Emergency Response Team), CIRC (Computer Incident Response Team).

SIEM software identifies data and sorts it into categories such as malicious activity, failed and successful logins, and other potentially malicious activity.

When the software identifies an activity that may pose a threat to the organization, alerts are generated that indicate a potential security issue. These alerts can be set as low or high priority using a set of predefined rules. For example, if a user account generates 20 failed login attempts within 20 minutes, this may be marked as a suspicious activity but set with a lower priority, as the user is more likely to have forgotten their login information. However, if the account has 120 unsuccessful login attempts within 5 minutes, it is more likely to be under attack and marked as a high severity incident *("What is SIEM? SIEM Defined, Explained, and Explored"*, Forcepoint.com, 2023).

SIEM solutions provide a powerful method for threat detection, real-time reporting and long-term analysis of audit records and security events.

Because SIEM solutions can collect audit records of events from multiple applications and devices, they allow IT security experts to identify, review, and respond more quickly to potential security breaches. Identifying the threat in the early stages ensures a mitigating effect.

Accident Response Systems – Detection and Prevention of Intrusion Attempts/IDS/IPS/IDPS

Intrusion detection is the process of monitoring events occurring in a computer system or network and analysing signs of possible incidents that are breaches or imminent threats of breaches of computer security policies, acceptable use policies, or standard security practices. Intrusion Detection System (IDS) is software that automates the process of detecting network intrusion attempts. Intrusion Prevention System (IPS) is software that has all the capabilities of an intrusion detection system and can also try to stop possible incidents. The term Intrusion Detection and Prevention Systems (IDPS) is used to integrate IDS and IPS technologies.

Many IDPS can identify intelligence, which may mean that an attack is imminent or that a particular system or system feature is of particular interest to attackers. Another application of IDPS is to gain a better understanding of the threats that are detected, using artificial intelligence technologies and analysing the frequency and characteristics of attacks. The aim is to be able to define appropriate security measures. Some IDPS may change their security profile when a new threat is detected.

IPS technology differs from IDS technology in the fact that IPS technology can respond to an open threat by trying to prevent its success. IPS systems have sensors operating in training or simulation mode (Petters, n.d.).

Along with these systems, the components of the information infrastructure of the cybersecurity system in organizations include video surveillance systems, next-generation firewalls and others.

The traditional firewall provides access control, i.e., check the status of network traffic. Next-generation firewall (NGFW) can block modern threats such as malware and application-level attacks.

It is necessary to conclude that the breaches and attacks nowadays impose the need to develop the ability to detect, investigate and mitigate the consequences of computer accidents. This is a reason to define the following option for the organization of the components of the information infrastructure of the cybersecurity system in organizations in cyber conflict environment. Two areas are considered: providing services and monitoring security events to prevent accidents.

The information infrastructure of the cybersecurity system in organizations includes the following component servers and workstations as an option: Security Information Event Management System (SIEM) for incident handling and analysis, Security Server; WAP (Web Application Proxy); DNS (Domain Name Server); Database Server for database; Active Directory (AD) – Domain Controller (DC) with Active Directory; e-mail server – Exchange Server; Logs Server for recording events; IDS/IPS (IDPS); NVR (Network Video Recorder) server for video surveillance; PBX (Private Branch Exchange – telephone system), web server with WordPress installation) etc., as well as workstations of security administrators, remote users. They are presented in *figure 1*.

In the architectural configuration of the components of the information infrastructure of the cybersecurity system in organizations for the term "*component*" the terms *functional configuration*, *platform* and *configuration* are also used.

The various components (platforms) of the information infrastructure of the cybersecurity system are considered as functional configurations. Each of them has a distribution of its elements into five layers: network services; kernel services; infrastructure services; common support application services and application services.

In this sequence, the functional configurations of the platforms (components) are defined, as shown in *figure 1*, as well as their system design. According to the concept of architectural configuration of the components of the information infrastructure, for each of the components the following descriptions or configurations are developed, which represent a different aspect – functional, technical and software configuration. For each of the three configurations a graphic and tabular design is being developed (*"Functional Configuration (FC) Template"* – NSV-12, *"Technical Configuration (TC) Template"* – NTV-3, *"Software Configuration (SC) Template"* – NTV-4), according to the templates[2] [(ISSC NATO Open Systems Working Group, AC/322(Sc/5)N268, 2002, pp. 49-67, Annex A] of the NTRM Concept.

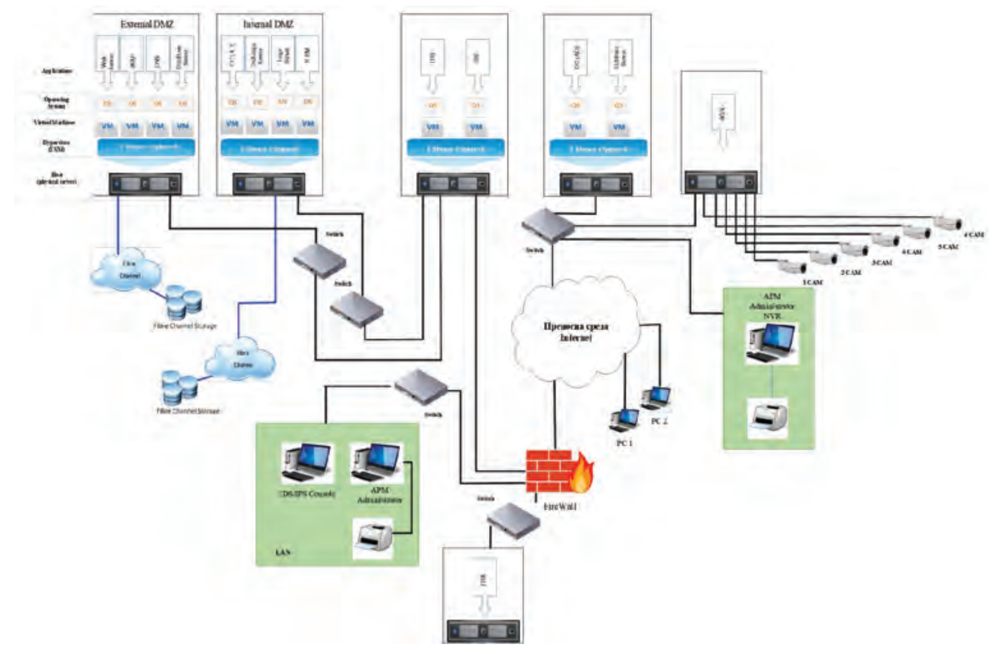


Figure 1: CIRT system information infrastructure components (authors' compilation)

ARCHITECTURAL CONFIGURATION OF A SERVER FOR PROCESSING AND ANALYSIS OF COMPUTER INCIDENTS – SECURITY INFORMATION EVENT MANAGEMENT (SIEM) SERVER

Functional configuration of the server for processing and analysis of computer incidents – Security Information Event Management (SIEM) is shown in graphical form, *figure 2*, and tabular view, *table 1*, which represents the *"Functional Configuration Template"* NSV-12, according to the architectural configuration concept. Functional configuration is built through the five layers of services previously listed: application services; common support application services; infrastructure services; kernel services; network services.

Elements of the following functional components are located in each of these layers: Management components; Network components; Application components; Basic components; Security components.

2 Annex A – NC3TA Compliance Templates includes NATO System View Template 12 (NSV-12) Functional Configurations, NATO Technical View Template 3 (NTV-3) Technical Configurations, NATO Technical View Template 4 (NTV-4) Software Configurations.

At the level of functional configuration, the SIEM architecture has been developed. It is presented in more detail with the technical and software configuration.

A technical configuration is a transition from a technical view to software configurations that define specific segments and their component and software products. The Internal and External Interoperability Profiles (IIPs and EIPs) are indicated here too.

The software configuration presents the software for executing the technical configuration. The components and standards used in the technical configuration are transformed into products and segments.

Functional Configuration of SIEM

In tabular form, template NSV-12, *"Functional configuration template"*, is used, which presents the functional services and interfaces *(Table 1)*.

Table 1: NSV-12 functional configuration (FC) template of the security information and event management server (SIEM) (authors' compilation)

NSV-12	FUNCTIONAL CONFIGURATION (FC) TEMPLATE		
Project title	CIRT INFORMATION SYSTEM		
Project POC	Name	Address	Tel/Fax/ Email
FC title	Functional Components of Security Information and Event Management SIEM		
FC Type *Note: Choose existing type, otherwise, create new child FC under one of the main categories, or create a new category*	SIEM SERVER Analysis, profiling, automation, and summarizing potential threats. Incident investigation, threat intelligence.		
FC Services at:	Foundation Services	Network Services	

Note: Describe the application services in functional terms	*Network Services Layer*	*Kernel Services Layer*	*Infrastructure Services Layer*	*Common Support Application Layer*	*Specific Mission Application Layer*
	Traffic Balancing Network stack	Configuration Control / Remote installation; Operation systems; Windowing software; Applications; Devices. Databases	Vulnerability scanning User information Asset information Threat intelligence	Data collection Correlation Normalization Data aggregation	Analysis applications Reporting applications Real-time monitoring applications Server applications
Functional Interface *Note: Describe the functional interface with other FCs in terms of required interoperability services (e. g.: email, authentication) and the required quality and quantity attributes (e.g.: no. of messages, security credentials) using the NSV1 (a-d), NSV3 and NTVI* templates	SSH[3] interface port 22 SMTP[4] interface port 25 RDATE[5] interface port 37 Port Mapper interface port 111 HTTPS[6] interface port 443 Syslog interface port 514				

[3] Secure Shell (SSH) is a cryptographic network protocol. See, for instance, https://www.ssh.com/, retrieved on 5 January 2024.

[4] Simple Mail Transfer Protocol (SMTP) is a TCP/IP protocol used in sending a dreceiving e-mail, https://www.smtp.com/, retrieved on 5 January 2024.

[5] RDATE is a get and possibly set the system date and time from a remote host for Unix OS e-mail, http://manpages.ubuntu.com/manpages/bionic/man8/rdate.8.html, retrieved on 5 January 2024.

[6] Hypertext Transfer Protocol Secure (HTTPS), https://www.ssl.com/faqs/what-is-https/, retrieved on 5 January 2024.

Technical Configuration of SIEM

The main purpose of the technical configuration is to determine the technological and technical standards that must be applied in the design and construction of the system. Technical configuration is a technical transformation of the functional configuration. It means that the application services that are described in the functional configuration are transformed into components with their basic standards. The internal and external interoperability profiles are also indicated here, which are developed both graphically *(figure 2, figure 3)* and tabular *(table 2)* in NTV-3 *"Technical Configuration (TC) Template"*.

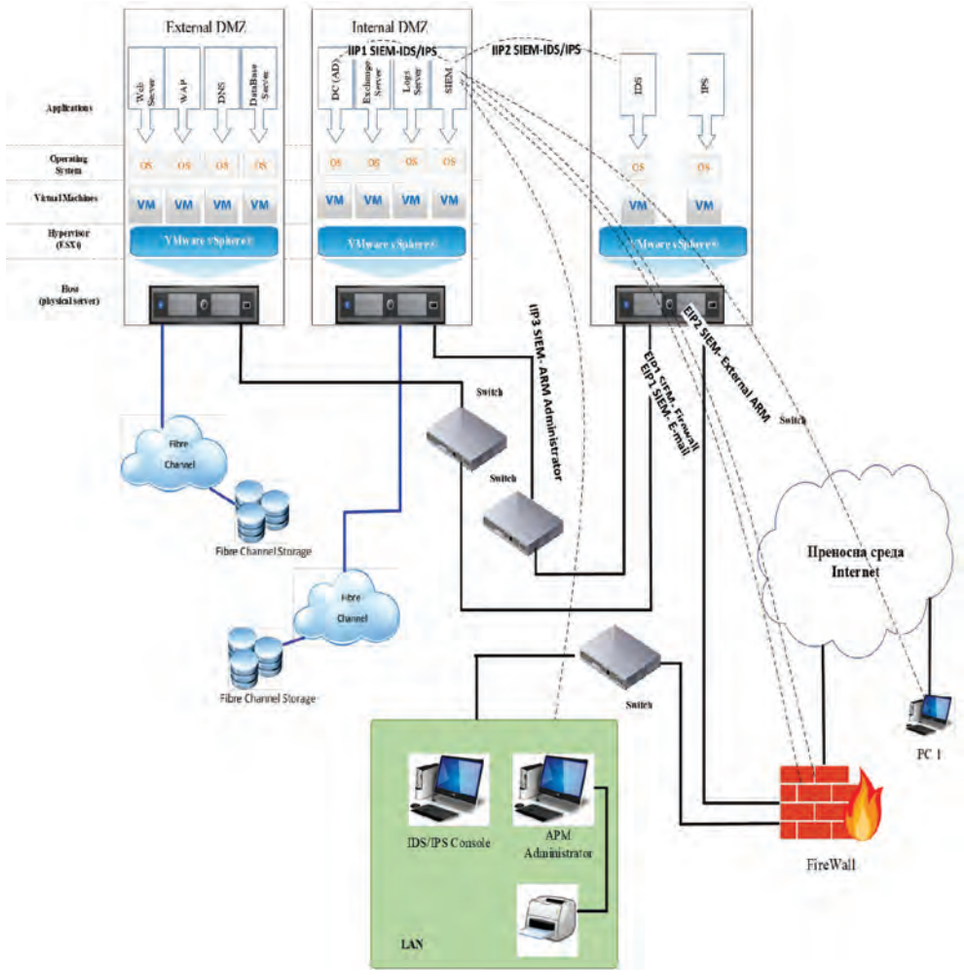


Figure 2: Technical configuration with interoperability profiles between the components of the information environment (authors' compilation)

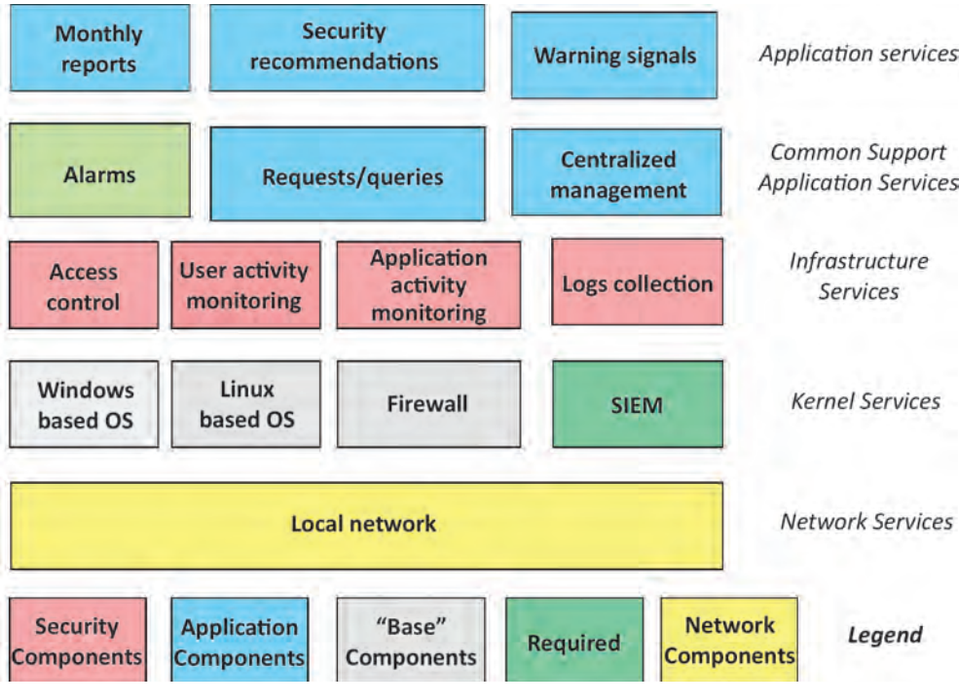


Figure 3: Graphic representation of the technical configuration of the SIEM server according to NCOECM (authors' compilation)

In technical configurations, internal interoperability profiles are defined within relevant protocols and standards. To allow flexibility in order to replace obsolete products with new ones, it is advisable to choose open standards and choose products that use such standards. The technical configuration is presented in *table 2*.

Table 2: NTV-3 technical configuration of SIEM server (authors' compilation)

NTV-3	TECHNICAL CONFIGURATION (TC) TEMPLATE (to be filled at Procurement Phase for Target Architecture)				
TC Components and Standards at: *Note: attach for each required component a detailed description*	*Network Services Layer*	*Kernel Services Layer*	*Infrastructure Services Layer*	*Common Support Application Layer*	*Specific Mission Application Layer*
	Local network	Windows based OS Linux based OS Firewall SIEM	Access control Identity management User activity monitoring Behaviour analysis Application activity monitoring Logs collection	Alarms Requests / queries Centralized management	Monthly reports Security recommendations Warning signals

Internal Interoperability Profiles (IIP) between TC and: *Note: Attach for each IIP a detailed description*	IIP1 – Active Directory Server – Domain Controller IIP2 – Server *"IDS/IPS"* IIP3 – Workstation for monitoring and administration of Windows OS
Interoperability Profile between TC and: *Note: Attach for each E1P a detailed description* EIP-Number and Basic Functionality: *Note: Use numbering as follows EIP<TCnr>-<TCnr>*	EIP1 – Firewall EIP2 – Workstation – A remote workstation for administering the Linux operating system (OS) EIP3 – Email Server

Internal Interoperability Profiles (IIP) are as follow:

- Profile IIP1 – Data exchange with a server active directory (Kerberos, LDAP[7], File Replication, Global Catalog, DNS)
- Profile IIP2 – Data exchange with a server IDS/IPS
- Profile IIP3 – Data exchange with the Windows OS workstation

Software Configuration of SIEM

As it has been already mentioned, the Software Configuration is a software implementation of the technical configuration. The software configuration consists of the real products that are used, which describe the software solution of the technical configuration. The software configuration represents the software for executing the technical configuration, which means that the components and standards used in the technical configuration are transformed into products and segments. The software configuration of SIEM is graphically presented in *figure 4*, and, in tabular form, in *table 3*.

[7] Lightweight Directory Access Protocol (LDAP) for interacting with directory servers and used for authentication and storing in formation about users, groups, and applications, https://ldap.com/, retrieved on 7 January 2024.

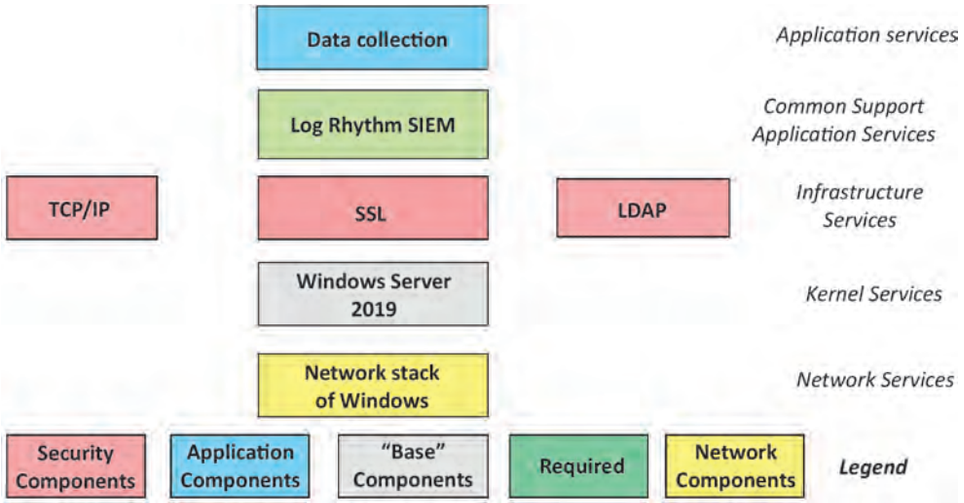


Figure 4: Graphical representation of SIEM software configuration according to NCOECM (authors' compilation)

Within the information environment, software packages, which are located horizontally in the graphical representation of the software configuration, are presented in separate units, also known as *segments*. The segments are similar in functionality to modules and can be easily added to any hardware platform. Segmentation gives the user the opportunity to choose from packaged and tested software components that are considered necessary in a particular situation. SIEM software configuration is developed in *table 3*.

Table 3: NTV-4 SIEM software configuration template (authors' compilation)

NTV-4	SOFTWARE CONFIGURATION (SC) TEMPLATE *(to be filled in the Procurement Phase for Target Architecture)*				
SC products in: *Note: Indicate software version number and standard(s) which are covered by the software package*	*Network Services Layer*	*Kernel Services Layer*	*Infrastructure Services Layer*	*Common Support Application Layer*	*Specific Mission Application Layer*
	Network stack of Windows	Windows Server 2019	TCP/IP[8], SSL[9], LDAP	Log Rhythm SIEM[10]	Data collection

[8] TCP/IP -Transmission Control Protocol/Internet Protocol.
[9] SSL – Secure Sockets Layer.
[10] Log Rhythm: SIEM Platform&Security Operations Center

Segments:	*Segment 1*	*Segment 2*	*Segment 3*	*Segment 4*	*Segment 5*
Note: Describe the products that constitute the different segments	Network stack of Windows	Windows Server 2019	TCP/IP, SSL, LDAP Log Rhythm	Data collection	
Interfaces	Internal	Internal	External	External	External
Interfaces *Note: Describe interfaces in terms of APIs embedded in products or as separate products; Mention the standards supported and possible parameter settings*	IIP1– UDP[11] port 88 for Kerberos[12] authentication IIP1 – TCP port 3268 and 3269 for the Global Catalog IIP1 – TCP and UDP port 53 for DNS[13] IIP1 – TCP 139 and UDP port 138 for file replication IIP1 – UDP port 88 for Kerberos authentication IIP1 – TCP port 3268 and 3269 for the Global Catalog IIP1 – TCP and UDP port 53 for DNS exchange IIP1 – TCP 139 and UDP port 138 for file replication IIP1 – TCP port 514 to collect logs EIP1 – Interface for exchanging information with Firewall EIP2 – TCP port 514 to collect logs EIP3 – TCP port 80 for web applications EIP3 – TCP port 443 for web applications EIP3 – TCP port 22 to exchange messages				

CONCLUSIONS

To develop the architecture of an organization's computer incident response centre, a proposal is offered to use NATO models to architecturally configure the components of the information infrastructure of cybersecurity systems.

It can be concluded that the authors have presented a methodology for application of NATO models for building information infrastructure in crisis conditions that includes architecture configuration and system design of its components in a specific way – by using NATO models. Various tools have been used, such as figures, tables and textual explanation. This presentation of the information infrastructure is not very popular among developers' teams, especially in the field of Resilient Information Systems design. We hope that the topic would be interesting because defining the information infrastructure and its software configuration could

[11] UDP – User Datagram Protocol.

[12] Kerberos is a network authentication protocol developed by the Massachusetts Institute of Technology. Introduction to Kerberos, https://www.ibm.com/docs/en/streams/4.2.1?topic=authentication-introduction-kerberos, retrieved on 7 January 2024.

[13] DNS – Domain Name Server.

successfully be used to improve the design of such systems in order to meet the challenges of crisis conditions environment.

ACKNOWLEDGEMENTS

This publication was financed by the Ministry of Education and Science in implementation of the National Scientific Program – Security and Defence that is funded by Ministry of Education and Science of the Republic of Bulgaria in implementation of National Strategy for the Development of Scientific Research 2017-2030, and was adopted by Decision of the Council of Ministers No. 731 of 21 October 2021.

BIBLIOGRAPHY:

1. Allied Data Publication 34 (ADatP-34) (n.d.). *NATO C3 Technical Architecture, Volume 2 Architectural Descriptions and Models* (Version 6.0). ISSC NATO Open Systems Working Group. Retrieved from NC3TA-Vol 2- v6.xml.
2. Demirov P., S. E. (2019). Informatsiya tai information natasreda, kato obekt za zashtita v cyber prostranstvoto. *Sborniktrudove NK, ISSN 1314-1937.* NVU "V. Levski".
3. ISSC NATO Open Systems Working Group, AC/322(Sc/5)N268. (2002). *NATO C3 Technical Architecture Implementation Handbook (NC3TA-IHB* (Vol. Version 1).
4. Introduction to Kerberos, https://www.ibm.com/docs/en/streams/4.2.1?topic=authentication-introduction-kerberos, retrieved on 7 January 2024.
5. Lightweight Directory Access Protocol (LDAP), https://ldap.com/, retrieved on 7 January 2024.
6. Petters, J. (n.d.). Varonis.com, https://www.varonis.com/blog/ids-vs-ips, retrieved on 9 August 2024.
7. Secure Shell (SSH), https://www.ssh.com/, retrieved on 5 January 2024.
8. Simple Mail Transfer Protocol (SMTP), https://www.smtp.com/, retrieved on 7 January 2022.
9. *"What is SIEM? SIEM Defined, Explained, and Explored".* (https://www.forcepoint.com/cyber-edu/siem, retrieved on 19 August 2024.
10. *"What Is SIEM?"*. (n.d.). Splunk.com, https://www.splunk.com/en_us/data-insider/what-is-siem.html#overview, retrieved on 7 January 2024.
11. Vasileva, V. (2020). Information Sharing Processes in Public Sector Cybersecurity Structures. *9th International Conference on Application of Information and Communication Technology and Statistics in Economy and Education,* pp. 136-147. Sofia: Publishing Complex – UNWE, http://icaictsee.unwe.bg/past-conferences/ICAICTSEE-2019.pdf, retrieved on 5 August 2024.

CYBER WARFARE
– THE NEW THEATRE OF WAR AND ITS LEGISLATIVE CLARIFICATIONS –

Marian-Valentin BÎNĂ, PhD
United Nations Support Mission in Libya
DOI: 10.55535/RMT.2024.4.16

This study aims to highlight the growing strategic importance assumed by the field of cybernetics in the dynamics of international politics. Cyberspace, an artificial environment created par excellence by human activity, has become crucial for power in the 21st century. After land, water, air and outer space, cyberspace represents the fifth dimension of new conflicts. In order to overcome these obstacles, I have chosen to clarify, from a legislative point of view, the status of this new dimension of conflict management. For the most part, official documents found in open sources define cyberwarfare as the use of incisive techniques for intrusion or sabotage an actor's information and physical resources, actions carried out in the context of a conflict, through the use of technology and telecommunications networks, which aim to compromise the defence, functioning, as well as the economic and socio-political stability of the adversary.

Keywords: cyberspace; cyberwarfare; information technology; lines of code; Tallinn Manual;

INTRODUCTION

In the modern digital age, every field of activity contains complex and novel technologies, and current combat actions confirm the prominent role of military intelligence and technology in achieving strategic, operational and tactical victory.

Considering traditional conflicts – on land, at sea and in the air –, which involve physical territories and tangible resources, a new front has in fact opened: the so-called *cyberwarfare*, which can be signified by the phrase *cyber theatre of war* (Shultz, 2022). The difference, the most important factor between this war space and traditional conflicts, is its substantially immaterial nature. The weapons used are lines of code, and the battlefield is made up of an infinite cyberspace, which, unfortunately, contributes, on the one hand, to a so-called democratization of information, and on the other hand, facilitates the possibility for malign actors to influence the target audience, through the narratives and information exposed.

EVOLUTION OF REGULATIONS APPLICABLE TO CYBERSPACE

In the international system, the concepts of *jus ad bellum* and *jus in bello* are those that regulate the potential use of force in a conflict. These normative and doctrinal developments, among others, represent the limitation of the behaviour of international actors and the imposition of restrictions, for example on the use of certain weapons, in order to prohibit attacks against specific targets or against the civilian population or to prepare the discipline that regulates the treatment that must be reserved for prisoners of war in addition to the roles, rights and obligations of the combatant. Thus, the provisions of the *Third Geneva Convention relative to the Treatment of Prisoners of War*, adopted in 1949, aim at the protection of prisoners of war, their rights and obligations in prisoner of war camps (Legislative Portal).

The genesis of these regulations is certainly not recent, and over the centuries they have evolved and adapted to the needs of the practical context, ultimately, of cyberspace. One of the first attempts to introduce a binding norm in international law on these issues took place with the establishment of the *Convention on Cybercrime from 2001* (Council of Europe, 2001), promoted by the Council of Europe, which, although it represented a starting point in the field, did not address the issue

of regulating the so-called cyberwarfare or the types of cyberattack inserted in the context of a hybrid war.

Undoubtedly, the legislative regulations made in this regard are found in art. 2 paragraph 4 and art. 51 of the Charter of the United Nations (Statuto delle Nazioni Unite, 1945). From the combination of their provisions, it is clear that states can undertake an act of self-defence when it comes to the use of force and when national security or territorial integrity is endangered. However, cyberspace raises new questions, such as, for example, regarding the existence and possibilities of extending the sovereignty of a country in cyberspace. The answer, although not exactly legal, but of an exclusively doctrinal nature, can be found in the *Tallinn Manual*[1], prepared by leading experts from the international academic world, specialists in international humanitarian law and military law. The manual essentially acts as a framework defining the categories of international law applicable to the cyber domain (Tallinn Manual 2.0). In this regard, the manual prescribes, in the first paragraph, that a country has the authority to exercise control over the entire cyber infrastructure and activities on its territory, with the inevitable consequence that, in the event of a cyber attack being detected, it may qualify it as an armed attack, expressly recognizing the possibility of defending itself (Ib.).

It seems appropriate to focus briefly on the *Tallinn Manual* which, as anticipated, does not have coercive effects for states, it only receives a kind of coercive effect through the lens of the main regulated reference notions. The importance of the regulations in question is found in the reinterpretation of existing international law, based on the undeniable dualism between the physical battle space (water, air, land) and the cyberspace. Although the infrastructure of cyberspace exists within territorial states through physical bodies containing data, their flow is only partially controllable by the state, which thus makes cyberspace immune to traditional ways of regulating the conflict context and, above all, although it is true that it is a new dimension, it is equally true that it cannot be considered separately from the three traditional dimensions mentioned earlier.

While the *Tallinn Manual* does not constitute a legislative regulation for states, it is a simple guide. The instruments that have legislative power are essentially international treaties and United Nations Security Council resolutions. For the latter, I believe it is appropriate to focus on the evolution of NATO legislation on the subject of cyberspace.

[1] The *Tallinn Manual* has become an influential resource for legal advisors and policy experts dealing with cyber issues. In many states, emerging state practice and public positions on international cyber law since the publication of the Manual necessitate an update of the 2017 edition. (A.N.)

NATO APPROACHES TO THE EVOLUTION OF CYBERSPACE

Although the North Atlantic Alliance has always protected its communications and information systems, it was not until the 2002 Prague Summit that *cyber defence* was included on the Alliance's political agenda. In 2006, the Riga Summit reiterated the need for additional protection of these information systems. In 2007, the well-known events in Estonia[2], which targeted a series of cyber attacks against public institutions, forced allied defence ministers to agree on the urgent need for intervention in this sector. It led to the approval of NATO's first cyber defence policy in January 2008. In the same year, the conflict between Russia and Georgia (Selene, 2018) demonstrated that cyber attacks can become a significant component of conventional warfare.

It was not until 2010, in Lisbon, that NATO developed a strategic concept in which it recognized that cyber attacks could become so severe that they threatened national and Euro-Atlantic prosperity, security and stability. Since April 2012, *cyber defence* has been introduced into the entire NATO defence planning process. In the following years, cyber warfare continued to be the subject of planning and consolidation on the NATO table, reaching approval at the 2014 summit in Wales (Damiano, Scatto, 2021), where the new cyber defence policy is recognized as an integral part of the defence system, thus allowing the use of force in the case of collective self-defence, according to the regulations of the United Nations Charter.

At the 2016 NATO Summit in Warsaw, Allied Heads of State and Government recognised cyberspace as an operational domain in which NATO must have the capacity to defend and respond (NATO, 2016).

Another crucial moment regarding the legislative regulation of cyberattacks took place at the 2021 NATO Summit in Brussels, where the new Cyber Defence Policy was approved, thus fulfilling NATO's core tasks, as well as its own general deterrence and defence tasks. It was expressly recognised that the impact of a clearly intentional attack in cyberspace must be considered an armed attack in all respects. In fact, it was precisely on that occasion that the 30 member states of the Alliance confirmed that, in the face of cyber attacks, Article 5 of the Treaty can be invoked and a new cyber defence policy was approved for a new approach to any

[2] In 2007, Estonia was the victim of a major cyberattack, affecting government websites, banks and information organizations. The attacker appears to have been Russia, although this cannot be confirmed with certainty. The first real cyberattack that took place in Estonia led to the need to expand the scope of Article 5 of the Atlantic Treaty, with the consequent legitimization of being able to resort to the collective self-defence mechanism. In the same context, the Cooperative Cyber Defence Centre of Excellence (CCDCOE), one of the largest centres of excellence of the Alliance, was established, located right in Tallinn. This centre aims to improve cooperation between member states in the field of cyber defence. (A.N.)

type of cyber threats, even low-level ones (Damiano, Scatto, ib.). At the next NATO summit in Vilnius in 2023, the member states approved a new scheme for improving cyber defence, regarding NATO's global defence and deterrence. The concept will further integrate the three levels of defence, namely:

- information technology defence;
- political, military and technical defence;
- defence regarding civil-military cooperation, in times of peace, crisis and conflict, as well as the commitment to collaboration with the private sector.

OTHER CLARIFICATIONS REGULATING CYBER WARFARE

As we have seen, the laws of war are more likely to be applied in a physical context, which is not as effective in the cyber domain, thus raising issues regarding the difficulty of identifying the attacker and the effectiveness with which this type of attack is characterized.

The classification of attackers is only one of the many problems in this field. In 2000, McConnell International produced a very interesting report examining crimes and attacks committed in cyberspace and the related penalties. Analysing the current state of the laws in 52 states, they found that only a small number of them had changed their legislation to address the various cyber attacks, but the main problem was represented by transnational cyberspace, since there can be major problems when a criminal cyber attack involves several nations (Cyber Crime Treaty, 2024; Soafer, Goodman, 2001, pp. 1-34).

In order to determine whether military intervention is needed, it is necessary to correctly identify the aggressor, because depending on who the attacker is, where the attack comes from and what is being attacked, different rules will be applied. In today's society, in cyberspace, criminals are becoming increasingly expert in the use of computer technology. Hacking tools, with video tutorials on how to use them, are freely available. So-called *"script kiddies"*[3] or people with little technical knowledge can already find the code written to carry out the desired actions. These attacks can range from simple, vandalistic attacks to well-thought-out operations against critical infrastructure. In this context, identifying the source of a cyberattack requires identifying the physical location of the attacking system, for example, tracing the attack and attributing it to a specific IP address, identifying the system or systems used, identifying the people responsible for the attack,

[3] A *script kiddie*, by definition, is a person without technical expertise who uses pre-existing automated tools or scripts to launch attacks on computer systems or networks, https://www.sangfor.com/glossary/cybersecurity/what-are-script-kiddies. (A.N.).

and possibly identifying the organization sponsoring it. In rare cases, all of these elements can be concentrated in a single subject.

Due to the need to integrate information from the commercial and government sides, intelligence and military agencies thus complicate identification and can lead to a significant delay in the investigation of the attack. In an environment where attacks can take place in less than a second and, especially, at zero cost, when you already have the appropriate electronic equipment, the placement of such attacks facilitates the spread and exponential growth of the number of subjects who can resort to such measures (Strouble, Carroll, 2008).

CONCLUSIONS: CHALLENGES AND PROSPECTS

Currently, there is still no complete set of regulations, thus raising a number of implementation problems for international law, first of all, identifying the moment when a state is allowed to resort to self-defence and, therefore, to the possible use of force, if it were the victim of a cyber attack.

The current legislative regulations regarding cyber warfare are lacking in the unfortunate situation of overcoming a crisis that, even tomorrow, unfortunately, could lead to dramatic events. The absence of predetermined standards for the assessment and reaction to cyber attacks, which are validly adopted by the member states of the European Union or by the member countries of NATO, could constitute the fundamental element of a possible defeat in cyberspace. We must hope that, perhaps, as soon as possible, Western governments, NATO, as well as other commercial entities can have homogeneous and timely resources and criteria to achieve uniform, adequate and sufficient defensive standards to counter any attack of a cyber nature.

As history has taught us, decisions that in some way limit national sovereignty can be difficult to implement, especially since any form of integration inevitably leads to an erosion of state sovereignty. Cyberspace should, however, be managed much more effectively if it is shared with other states or members of international organizations.

Perhaps we could go so far as to say that national integration, rather than a possibility, should be considered an inevitable and mandatory requirement for defensive validity, precisely because cyberattacks could produce harmful effects comparable to physical attacks, with widespread consequences. It is necessary and indispensable that possible conduct should be identified and codified without delay by states and international actors, implemented at the level of cyberspace and reinterpreted on the basis of the legislation in force.

Therefore, it is now clear that cyberspace represents the opening of a new front, which must be taken into account. Despite the fact that NATO has declared the possibility of invoking Article 5 in the event of a cyber attack against any member of the Alliance, this situation requires a precise and concise assessment, carried out by relevant, unambiguous methods. The lack of predetermined standards for assessing cyber attacks could pose problems for NATO member countries, which have different internal methods to counter them. To overcome this ambiguity, it would be desirable for NATO to adopt uniform standards to assess individual cyber attacks and to determine whether they have reached a level of increased severity that would make it an armed attack.

According to what is presented in this article, we can say that the laws of war are applied rather in a physical context, not being as effective in the cyber domain, raising, as such, problems regarding the difficulty of identifying the attacker and the efficiency that characterizes such type of attack.

BIBLIOGRAPHY:

1. Brown, G., Poellet, K. *The Customary International Law of Cyberspace.* In *Strategic Studies Quarterly*, http://www.jstor.org/stable/26267265, retrieved on 2 August 2024.
2. *UN Charter* (1945), https://www.miur.gov.it/documents/20182/4394634/1.%20Statuto-onu.pdf., retrieved on 12 June 2024.
3. *Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 14 June 2021*, Brussels Summit, https://www.nato.int/cps/en/natohq/news_185000.htm, Press Release (2021) 086, published on 14 June 2021, updated on 1 July 2022, retrieved on 22 August 2024.
4. *Council of Europe* (2001). *Convention on Cybercrime*, https://www.coe.int/it/web/portal/home (STE no. 185), https://rm.coe.int/1680081561, retrieved on 27 May 2024.
5. *Council of Europe action against Cybercrime*, https://www.coe.int/it/web/portal/coe-action-against-cybercrime#:~:text=La%20Convenzione%20sulla%20criminalit%C3%A0%20informatica%20(2001)%20%C3%A8%20l'unico,tra%20i%20suoi%20Stati%20parti, retrieved on 22 June 2024.
6. *Cyber Crime Treaty*. Global Information Assurance Certification Paper, https://www.giac.org/paper/gsec/839/cybercrime-treaty/101761, retrieved on 22 June 2024.
7. *Cyber defence*. *NATO*, https://www.nato.int/cps/en/natohq/topics_78170.htm, retrieved on 2 August 2024.
8. Damiano, L., Scatto, E. *Nato, la nuova "Cyber Defence Policy": ecco le priorità dell'Alleanza nella difesa dello spazio cibernetico*, https://www.agendadigitale.eu/sicurezza/nato-la-nuova-cyber-defence-policy-ecco-le-priorita-dellalleanza-nella-difesa-dello-spazio-cibernetico/, retrieved on 12 June 2024.
9. *Manualul Tallinn* 2.0. CyberLaws, https://www.cyberlaws.it/2019/manuale-tallinn/, retrieved on 22 August 2024.
10. NATO (2016). *Cyber defence,* https://www.nato.int/cps/en/natohq/topics_78170.htm., retrieved on 22 August 2024.

11. Pool, P. (2013). *War of the Cyber World: The Law of Cyber Warfare. The International Lawyer*, source: http://www.jstor.org/stable/43923953, retrieved on 22 August 2024.
12. Portal legislativ/Legislative Portal, https://legislatie.just.ro/Public/DetaliiDocument/255597, retrieved on 12 August 2024.
13. Sironi de Gregorio, F. (2019). *Il Manuale di Tallinn 2.0.*, CyberLaws, https://www.cyberlaws.it/2019/manuale-tallinn/, retrieved on 12 July 2024.
14. Shultz, N. (2022), https://www.fordhamilj.org/iljonline/cyber-warfare-the-newest-theater-of-war, retrieved on 22 July 2024.
15. Soafer, A., Goodman, S. (2021). *Cyber Crime and Security. The Transnational Dimension.* In *The Transnational Dimension of Cyber Crime and Terrorism*, vol. Hoover Institution's National Security Forum Series, pp. 1-34, California: Hoover Institution Press, https://www.hoover.org/sites/default/files/uploads/documents/0817999825_1.pdf, retrieved on 22 August 2024.
16. *Statuto delle Nazioni Unite* (1945), https://www.miur.gov.it/documents/20182/4394634/1.%20Statuto-onu.pdf; Organizzazione delle Nazioni Unite, https://www.miur.gov.it/documents/20182/4394634/1.%20Statuto-onu.pdf, retrieved on 27 May 2024.
17. Strouble, D., Carroll, M. (2008). *Law and Cyber War*, SAIS 2008 Proceedings, http://aisel.aisnet.org/sais2008/37, retrieved on 12 July 2024.
18. *The North Atlantic Treaty* (4 April 1949. Washington D.C., https://www.nato.int/cps/en/natohq/official_texts_17120.htm, retrieved on 22 June 2024.
19. Verri, S. (8 August 2018). *La guerra dimenticata: sintesi e analisi del conflitto russo-georgiano 10 anni dopo.* Euronews, https://it.euronews.com/2018/08/08/la-guerra-dimenticata-sintesi-eanalisi-del-conflitto-russo-georgiano-10-anni-dopo, retrieved on 12 July 2024.
20. https://www.sangfor.com/glossary/cybersecurity/what-are-script-kiddies, retrieved on 22 August 2024.

THE PEOPLE'S REPUBLIC OF CHINA AND THE THREATS TO NATO'S CYBER SECURITY

Lieutenant Colonel (N) Claudiu-Cosmin RADU, PhD Student
"Carol I" National Defence University, Bucharest
DOI: 10.55535/RMT.2024.4.17

In recent years, many NATO member states have reported violations of cyber sovereignty, accusing the People's Republic of China (PRC). PRC has its own vision of cyberspace, employing technological advances to strengthen its position as a global leader. This article addresses NATO's cyber security challenges, analysing how Beijing's actions influence international politics and cyber stability. Utilizing a combination of qualitative and quantitative analysis, the research explores the ways in which the PRC pursues its geopolitical goals in cyberspace, as well as NATO's response measures. From the analysis of cyber security policies, we draw insights into the strategic directions each side is pursuing. The article also assesses the long-term impact of cyber tensions between the PRC and NATO and exposes the importance of international collaboration in promoting a stable and secure cyberspace. The conclusions emphasize the need for a coordinated and proactive approach to counter cyber threats and strengthen the Alliance's cyber defence.

Keywords: People's Republic of China; cyber security; NATO; cyber threats; cyberspace;

INTRODUCTION

The accelerated progress in information and communication technology in recent years has been of significant importance in the development of cyber capabilities worldwide. With this technological advancement, the People's Republic of China, hereafter referred to as the PRC, has become a major force not only economically and militarily, but also in cyberspace, strengthening its presence in this key area of international security. In the context of these developments, NATO, the alliance of Western democratic states, is facing unprecedented challenges posed by aggressive cyber-aggression in cyberspace. In the view of the member states, the main countries funding non-state actors or conducting offensive cyber activities are considered to be the Russian Federation, the People's Republic of China, North Korea and Iran (Diotte, 2020).

The PRC's expansion into cyberspace has attracted the attention of major Western powers, especially the United States of America, which sees Beijing as the main cyber security threat. According to reports by NATO and other international organizations, the PRC has developed complex cyber espionage strategies, using sophisticated methods of infiltration and intelligence collection to gain economic, military, and geopolitical advantages (Hamilton, 2020). The PRC is increasingly manifesting its influence in cyberspace through policies and strategies specifically designed and tailored to achieve sovereignty in cyberspace. Its conception of this operational domain is considered innovative and forward-looking, as it views cyberspace as a virtual extension of its territory, which it seeks to control in the same way it manages its physical territory. This approach creates particular challenges for the North Atlantic Alliance, which promotes a free, open, peaceful and secure cyberspace and strives to increase stability and reduce friction between countries. These goals are intended to be achieved through international law and accepted norms of responsible state behaviour in cyberspace (NATO, 2024).

The PRC's cyber strategy focuses on deterrence and coercion in cyberspace (Hamilton, ib.), where Beijing conducts offensive actions against government entities and critical infrastructures of its adversaries, including NATO member states. This tactic is part of a broader strategy of geopolitical influence, through which the PRC seeks to expand its presence and consolidate its status as a global power.

The PRC's intense cyber activities are one of the main concerns for NATO, due to the complexity and high frequency of cyber attacks launched. These attacks range from DDoS (Distributed Denial of Service) attacks to sophisticated infiltration of government, civilian or even military networks, with the aim of weakening networks and obtaining information critical to national security. The big challenge for NATO is to strengthen its defences against these increasingly advanced cyber attacks. In this context, the Alliance has implemented initiatives to foster coordination and cooperation among member states in the field of cyber security. However, the PRC's rapid advances in cutting-edge technologies, such as artificial intelligence and quantum computing, are amplifying the complexity of this landscape, prompting NATO to intensify its efforts to develop more effective countering techniques.

The main purpose of this paper is to analyse the cyber developments and activities of the PRC and their impact on the security of the North Atlantic Alliance. In this context, the proposed objectives are: to analyse the tactics employed by the PRC in cyberspace and to correlate the North Atlantic Alliance's responses to counter PRC threats in this environment. Furthermore, the paper also aims to analyse the long-term implications of this cyber conflict and how international alliances can play a decisive role in maintaining global security in the digital age.

The research methodology consists mainly of qualitative methods, but includes some quantitative methods by analysing the content of laws, strategies and policies governing cyberspace in the PRC and NATO, as well as the scientific literature. Based on this analysis, the present study aims to answer the following research question: *Is NATO prepared to effectively counter the increasingly sophisticated cyberspace actions initiated by the PRC?*

The content analysis of the Beijing administration's cyber policies underlines its intention to use cyberspace to achieve its geopolitical, economic and national security ambitions. A strategy that integrates technological advancement with rigorous domestic control, cyber sovereignty and information control, are critical for Beijing, both for maintaining domestic stability and for expanding its global influence. At the same time, the PRC's ability to offensively develop and deploy advanced technologies poses significant risks to global cyber security, requiring a coordinated response from NATO and its partners.

THE EVOLUTION AND PERSPECTIVES OF THE CYBER POLICIES OF THE PEOPLE'S REPUBLIC OF CHINA

To understand the actions of the PRC in cyberspace, it is essential to analyse some of the motivations and goals behind these actions. It is not intended to justify the PRC's behaviour, but to provide insight into the factors influencing the decisions and strategies adopted. After the end of the Cold War, when there were basically two major centres of power, new international actors emerged to claim their authority in various areas. As these new powers asserted their influence, many of them, including the PRC, experienced a rapid rise in areas such as technology, economics and military power. The PRC, with clear ambitions to become a major player in the global economy, has invested heavily in the development of advanced technologies, as it seeks to consolidate its geopolitical influence and reduce its dependence on other states. This global competition, fuelled by the egos and political ambitions of China's leaders, has led to an accelerated pace of research and innovation in emerging technologies such as artificial intelligence, 5G and 6G technology, Internet of Things (IoT) and quantum computing. In this context, the PRC has quickly recognized the value and potential of cyberspace, not only as a medium for economic development, but also as a strategic area for gaining competitive advantage over other states, whether through cyber espionage, intellectual property theft, or attacks on critical infrastructure (Chafetz, 2023). These actions are motivated by the PRC's desire to expand its global influence, protect its economic interests, and position itself as an international technological leader. Through this aggressive, politically and administratively driven approach, Beijing seeks not only to assert its supremacy in cyberspace, but also to consolidate its role as a global power capable of influencing the international order and asserting itself in an increasingly competitive geopolitical landscape. These actions are deeply rooted in the autocratic structure of the state, which favours centralized control and the subordination of economic and legal interests to the Communist Party.

Over the past decade, the overall competition between the People's Republic of China and the United States of America has intensified significantly, and a new front of this rivalry has emerged in cyberspace. In this context, both countries accuse each other of cyber espionage, unfair competitive practices and interference in national critical infrastructures. Critical infrastructure, which includes electricity grids, transportation systems and communications, is a particularly sensitive national asset and the security of these systems is essential to the functioning of any modern nation. Moreover, intrusion into these networks is perceived as a threat

to national security and is addressed by most states in their national strategies and cyber security strategies.

Much of the tension in cyberspace between the PRC and the USA centres on accusations of espionage, both in the military and economic spheres. Although both nations accuse each other of extensive espionage, the practice is not limited to just the two states. Most NATO member states have experienced a wider range of cyber incidents from state or non-state actors with ties to the PRC. Paradoxically, the complexity and economic interdependencies between states lead to a certain caution in carrying out such actions. Nonetheless, competition continues to be waged through DDoS attacks, infiltration of government institution networks and disinformation influence campaigns, all of which fall within the boundaries of hybrid warfare. However, cyberattacks are often considered a component of contemporary diplomatic and military strategy without escalating the threshold that would trigger direct armed conflict (Jinghua, 2019).

Beginning in the 1990s, the PRC began to understand the profound impact that new technologies could have on the future. Officials in Beijing saw the potential of developing cyber capabilities, first for their low cost, and second for the efficiency with which they could replace conventional technologies. Internet networks were put under tight control as the leadership was concerned about controlling access to the internet and digital infrastructure. There were fears that the country could become vulnerable to attacks from other nations, which had already begun to integrate advanced digital solutions into their military strategies (Jiang, T., 2022).

This period has been one of consolidation, influenced by military conflicts in which advanced technologies for the time were used in conflicts such as the 1991 Gulf War, which served as a clear demonstration of American technological advantage. The conflict is considered by many analysts as the first *"computerized war"* due to its extensive use of modern technologies such as advanced communications systems, radar, satellites, and guided weapons. Essentially, electronic warfare techniques were used to disrupt and intercept Iraqi communications as well as to precisely coordinate attacks. Although no actual cyber-attacks were launched, the war demonstrated the increasing reliance on cyber technologies in warfare, foreshadowing the importance of cyberspace actions in future conflicts. It was only during the Kosovo conflict in 1999 that cyber-attacks were employed, marking the event as the first *"internet war"*. Governmental and non-governmental actors alike used the internet to disseminate information, spread propaganda, spread fake news and solicit support for their positions (Denning, 2001). In the wake of global events,

the PRC perceived the need to accelerate its own cyber capabilities as a preventive measure. At the same time, the groundwork is being laid to strengthen control over the PRC's national cyber infrastructures. The ambitions for cyberspace security are heavily shaped by the trajectory of the PRC's informatization strategy. In 2000, it set the goal of becoming an advanced information society, where businesses, scientists, and citizens use the latest information and communication technologies (ICTs) to improve performance and enhance social benefits (Austin, 2018, p. 11).

At the national level, cyber research and development has been stepped up to secure its territory against external threats. Moreover, Beijing's strategy focuses heavily on *"network sovereignty"*, which translates into the government's ability to control the flow of information on the internet. It has included the implementation of strict censorship and data traffic monitoring measures designed to prevent external infiltration and protect national interests (Jiang, T., ib.). According to the same author, since 2008, the PRC has become the largest internet market in the world with over 253 million users. This rapid expansion of the internet has coincided with its rise to the global economic podium. However, the growth of the internet has not only been an engine of economic growth, but also a source of vulnerabilities, and it has become increasingly focused on the dangers associated with cyber security. Above all, the state has begun to realize the need to protect its critical infrastructures, such as financial institutions and energy grids, against potential threats from cyberspace. Like most countries, the PRC is heavily dependent on technology, prompting the government to closely monitor developments related to the internet and the flow of information it generates. The Chinese authorities perceive uncontrolled information as a threat to the regime and make considerable efforts to take advantage of the economic opportunities offered by the internet while maintaining political control over it (Grauman, 2012).

In this context, the Chinese Communist Party perceived the Internet as a threat to the regime's stability, given the possible impact of external influences on the Chinese population. To combat these risks, the PRC began in 1998 to develop a strategy based on surveillance and restricting access to information. A key first step was the launch, in 2003, of the *Golden Shield Project*, the basis of the *PRC's "Great Firewall",* which allows the regime to censor online content and block access to foreign information sources deemed harmful or subversive. The project is intended to filter and control internet traffic, blocking access to content outside the country's borders that is deemed sensitive (Austin, p. 11), effectively isolating the national internet from the global internet. In other words, the authorities combine digital

censorship with social surveillance, allowing them to track and control citizens' online behaviour. As part of this project, since 2009, the PRC has made efforts to block certain US software applications (such as Facebook, Twitter and YouTube) because of their incompatibility with its censorship laws (The International Institute for Strategic Studies, 2021).

To ensure regulatory compliance, the project also integrates digital identification measures whereby citizens are obliged to use real names on online platforms as a goal of maintaining cyber security (Triolo, Sacks, 2017). Users thus become directly responsible for their online activities, reducing the possibility of anonymous dissent and increasing self-censorship. Moreover, the *Golden Shield* has thus become a central pillar in the PRC's cyber strategy, setting standards for control and internet censorship. It thus marks a fundamental aspect of the PRC's broader cyber security and information sovereignty policies, establishing a model for a state-controlled internet that closely aligns with national security priorities. This framework is critical for understanding the development and implementation of Chinese cyber policies in the future.

After 2007, several events took place in cyberspace. Russia was accused of using cyberspace for offensive actions against Estonia and Georgia, and the USA was accused of being behind the Stuxnet attack. Moreover, the uprisings during the Arab Spring underlined the importance for the PRC to strengthen its cyber capabilities in order to protect its critical infrastructure and maintain national stability. The Stuxnet incident demonstrated the vulnerabilities of industrial networks to sophisticated attacks, prompting the PRC to reassess cyber strategies to prevent such threats. During this period, the USA recognized cyberspace as a new operational domain in addition to land, air, sea, and space (The White House, 2011). This recognition emphasized Beijing's focus on technology development to protect national interests and maintain internal security in an increasingly complex global landscape. Consequently, during this period, as the PRC rose to become the world's second-largest economy, its political, economic, and social development became deeply intertwined with global cyberspace (Jiang, T., ib.).

In 2010, the PRC published a White Paper on the status of IoT, emphasizing the need for cyber security to protect national security and state interests within its sovereign territory (Hwang, 2023), which reveals the recognition of the importance of cyber security in the context of national security. A year later, the PRC together with other states, including Russia, Tajikistan and Uzbekistan, presented an *International Code of Conduct for Information Security* to the UN General Assembly.

It reaffirmed the belief that rights and decision-making responsibilities for Internet-related public policies should be under the jurisdiction of the host state (United Nations General Assembly, 2011).

A new stage in the PRC's cyber security was ushered in when the country's President Xi Jinping announced the country's intention to become a cyber power. He initiated a series of institutional changes to achieve this goal. One of the most significant developments was the establishment of the *Cyberspace Administration of China* (CAC) in 2014. This institution becomes responsible for regulating, administering, and licensing the Internet in the PRC. The official view in the PRC, as in most rich and middle-income countries, is that cyber security affects and shapes the entire range of government, economic, social, technological, political, and security activities in the country (Austin, p. 7).

In 2015, the *China Information Technology Security Evaluation Centre* was established under the CAC with a role in strengthening national defence against cyber threats. Through its research work, the centre has provided key insights and strategies for effectively protecting the PRC from cyberattacks (Jiang, T., ib.). Also in the same year, the government issued new regulations targeting foreign IT companies that supply Chinese banks, requiring them to disclose the source codes of the IT products they supply. The measure was imposed to strengthen both domestic cyber security and localization of the cyber security industry (Austin, p. 14). The response came along political-diplomatic lines when PRC-USA bilateral relations cooled, prompting the PRC to suspend the measures also in the same year.

As the internet and cyber technologies have become an essential part of the economy and national security, the PRC's strategy has evolved from control and offense to defence and deterrence. Against this backdrop, Beijing has adjusted its policies to address both internal and external challenges, focusing on preventing cyberattacks and protecting its critical infrastructure. Its ascent as a cyber superpower has been marked by a transition from aggressive expansion to strategic protection as it has become more deeply integrated into the global economy. Since 2015, the PRC has begun to adopt a more defensive posture in its cyber strategy. While in the early stages the strategy was focused on pre-emptive attacks and strengthening cyber sovereignty, gradually the focus shifted to defence and deterrence (Jiang, T., ib.). This shift reflects a growing awareness of the risks of large-scale cyber warfare and its associated economic and political costs (Soesanto, 2022).

Politically, the current Chinese administration has fully recognized the importance of cyber security and declared it part of national security. As a result,

it has issued several national laws and strategies to strengthen the country's cyber defence capabilities. The 2015 *National Security Law of the People's Republic of China* provides the general framework for national security and cyber security (Jiang, M., 2020). Moreover, Article 25 of the *National Security Law* emphasizes the importance of scientific development, innovation and national control over core information technologies, critical infrastructures, important information systems and data. It also sets goals of preventing, stopping and managing cyber-attacks, network intrusions, cyber-theft, online distribution of compromising information, ultimately leading to achieving security and sovereignty in cyberspace. In terms of the cyber strategies published by the Chinese Cyberspace Administration, the *International Strategy for Cyberspace Cooperation,* approved in 2016, stands out as the PRC seeks to take the lead in international cyber governance, following President Xi's call to *"establish a community of common future in cyberspace"* (Jiang, M., ib.). This strategy particularly emphasizes the principles of peace, sovereignty, shared governance and upholds peace through cooperation and strategic mutual trust.

At the national level, several institutions have implemented laws or issued policies on personal data protection, administrative regulations or rules on information activities in cyberspace. In terms of criminal activity, China's Criminal Law has been revised several times in 2005, 2009 and 2015 to reflect the increase in criminal activities involving personal information. The 2017 *Cyber security Law* of the PRC similarly contains several provisions regulating the collection, storage, transmission and use of *"personal information"* by network and critical information infrastructure operators (Jiang, M., ib.). This law was created to protect national network infrastructure and control the activities of foreign companies in Chinese cyberspace. The law requires companies to implement strict security standards and report information about vulnerabilities in their networks to the authorities. We can say that this law reiterates the concept of cyber sovereignty as a national security tool.

In terms of cyberspace as an operational domain, the Beijing administration is publishing *China's National Defence in the New Era* White Paper in 2019. This lays out an assessment of the current national and international security situation and outlines the PRC's defence missions, reforms, and spending. This paper provides a detailed analysis of the current state of national and international security, outlining the PRC's missions, reforms, and spending in the defence sector. Moreover, it emphasizes the need for the Chinese military to adapt to the *"new era"* of strategic competition by improving training and increasing combat capabilities, thus aligning

with the PRC's global status, as well as its commitment to maintaining *"world peace"*. In the area of cyber defence, the White Paper highlights Beijing's interest in adopting the most advanced technologies in the military sector, including artificial intelligence, big data, cloud computing, quantum computing and the internet of things (IoT) (The State Council Information Office of the People's Republic of China, 2019). In addition, the military modernization program entails a *"civil-military fusion"* strategy, strengthening the relationship between civilian companies and defence establishments. Through this fusion, the Chinese military could benefit from technological advances in many areas, such as nuclear technology, aerospace, aviation, semiconductors, cloud computing, robotics, and Big Data processing (Ford, 2019).

Similar to other states, the PRC aims to dominate cyberspace while recognizing the need for a substantial transformation of its armed forces to achieve this strategic goal. President Xi Jinping and his team have laid the groundwork for transforming the People's Liberation Army (PLA) into a *"world-class army"* by 2050. Achieving it depends on the state's ability to adapt emerging technologies and artificial intelligence to existing military doctrine (Burke, Gunness, Cooper III, Coza, 2020). Further, the authors expound that the PLA Strategic Guidelines emphasize the importance of cyberspace as an operational domain and a critical tool in the conduct of military operations in an era dominated by confrontation between *"information-driven systems of systems"*. In this context, one of the most important developments in the field of *"informatization"* is the establishment of the PLA Strategic Support Force, a structure dedicated to coordinating all information aspects of warfare, including cyber attack and defence as well as electronic warfare. These state structures may be joined by other forces specially trained to conduct offensive or defensive actions in cyberspace such as state-sponsored state actors, non-state actors or even patriots acting out of their own convictions.

For the future, the PRC aims to develop the digital infrastructure globally, creating economic and thus political dependencies for many countries. This strategy strengthens the PRC's role as a global player and gives it considerable influence in international decision-making processes, especially in relation to its policies on Taiwan. As the US Ambassador-at-Large for Cyberspace and Digital Policy pointed out in 2023, the PRC's strategy to build the global internet infrastructure – from fibre optics and satellites to data centres and wireless technology – shows that focusing solely on data and application security would ultimately mean *"delivering highly secure and uncorrupted packages directly to Beijing in an untrusted architecture"* (Hamilton, 2024).

NATO POLICIES IN CYBERSPACE

NATO has had a significant evolution in its policy and vision in cyberspace. The analysis of the evolution of NATO's cyber policy reflects a continuous adaptation to the increasingly complex and diverse threats in the digital environment. Starting from the Cold War, where global power had a bicephalous component, we arrive at the contemporary situation where the *"Thucydides trap"* may be more valid than ever. As the PRC, the Russian Federation or any other country seeks to become increasingly influential on the global stage, there are fears that economic, cyber, military or geopolitical frictions could escalate into a major conflict, although there is also the possibility of avoiding them through diplomacy and cooperation. Thus, the concept highlights how risky the geopolitical landscape can become when a rising economic, military or other nation challenges an established one.

Whether it is the PRC or NATO, their actions in cyberspace are closely linked to their history and political leadership. For example, the autocratic regime in Beijing seeks to control and censor activities in cyberspace, while NATO advocates a common, open and secure cyberspace. Cyber security and cyber defence are part of NATO's core mission of collective defence. Its main objectives in this area are to protect its own networks, to operate in cyberspace, to help allies build resilience to protect national networks and to provide a platform for consultation and collective action.

NATO's cyber security policy direction is being driven by the growing threat of state-sponsored cyber attacks. In response, North Atlantic Organization member states are increasingly adopting active cyber defence strategies. These combine real-time attack detection with proactive countermeasures to reduce potential damage. The United States and the United Kingdom are leading the way in their implementation, using technical and policy responses, including hackbacks, to deter and attribute cyber threats (Jun, 2023).

Cyber defence appeared on NATO's agenda at the *Prague Summit* in 2002 and was subsequently confirmed as a priority in 2006 at the *Riga Summit*. For the first time a policy was agreed by Heads of State and Government at the *Bucharest Summit* in April 2008. The rapid evolution, sophistication and increasing frequency of cyber threats and attacks to the Alliance's security have put the issue back on NATO's security agenda. The Strategic Concept adopted at the *Lisbon Summit* in 2010 recognizes that attacks in cyberspace can affect the security of national critical infrastructures and jeopardize *"national and Euro-Atlantic prosperity, security and stability"* (NATO Strategic Concept, 2010) and their impact could be as damaging

as a conventional attack. Accordingly, Lisbon laid the foundations for the Alliance to develop the capacity to prevent, detect, defend against and recover from such threats.

In 2014, at the *Welsh Summit,* no one denied that cyberspace operations could have an impact equal to that of conventional attacks. Moreover, for the first time, it was recognized that a member could invoke Article 5 following a cyber attack of significant magnitude, similar to those faced by Estonia in 2007. Following these cyber attacks in Estonia, NATO approved its first cyber defence policy in 2008 and established the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn.

At the Munich Security Conference in 2011, NATO adopted a new cyber defence policy that focuses on preventing cyber attacks and building resilience. The creation of the Rapid Response Team was the result of the review of the Alliance's cyber defence policy, as well as the implementation of a cyber defence capability of its own networks (Hasanov, Iskandarov, Sadiyev, 2019). As a result of the lessons identified and learned from cyber threats and attacks to date, the major powers have stepped up their activity in the digital environment concomitant with the development of laws, strategies, policies, and doctrines regulating the activity.

As a consequence of cyber activities to that point, in July 2016, at the *Warsaw Summit*, the Allies recognized cyberspace as an operational area in which NATO must defend itself as *"effectively as in the air, on land and at sea"* (NATO, 2016). The Allies agreed on a military vision and strategy for cyberspace operations and committed to prioritize action to strengthen national cyber capabilities by making a political commitment to do so *(Cyber Defence Pledge*), to increase the resilience of national networks and infrastructure, and to improve the responsiveness, responding quickly and effectively to cyber attacks. Predictably, at the *2018 NATO Summit in Brussels*, the Allies agreed to establish a *Cyber Operations Centre (CYOC)* as part of NATO's consolidated command structure. They also agreed that NATO can draw on member states' national cyber capabilities for Alliance operations and missions. A year later, in February 2019, the Allies endorsed a NATO Guidance that sets out a range of tools (political, diplomatic, military) to strengthen NATO's ability to respond to malicious cyber actions (NATO, 2024).

At the *2023 NATO Summit* in Vilnius, the Allies adopted a new *Concept* aimed at enhancing the Alliance's contribution to cyber defence and deterrence. Alliance members also reaffirmed and strengthened their commitment to cyber defence, setting more ambitious goals for strengthening national cyber defences, including

critical infrastructure. Recognizing the need for rapid assistance, NATO has initiated the *Virtual Cyber Incident Support Capability* to assist national efforts to mitigate significant cyber incidents (NATO, 2023). It is interesting that the name of the People's Republic of China appears twice in the communiqué preceding the Summit. The coercive interests and policies of the People's Republic of China are recognized as directly challenging international interests, security and values. The PRC uses a variety of political, economic and military tools to expand its global influence and project power. It also conducts harmful hybrid and cyber operations, uses aggressive rhetoric and practices disinformation, targeting allies and compromising the security of alliances. The PRC seeks to dominate key technological, industrial and critical infrastructure sectors and control strategic materials and supply chains. It uses economic leverage to create strategic dependencies and increase its influence, striving to undermine the rules-based international order, including in the space, cyber, and maritime domains (Ib.). Also in the same communiqué, it is stated that instability in Africa and the Middle East directly affects the security of both NATO and partners. The Alliance is facing cyber, space, hybrid and other asymmetric threats, and the clear intentions and coercive policies of the Beijing government defy NATO's interests and jeopardize its security (Ib.). Practically, as of this moment, the People's Republic of China is officially recognized by NATO as, if not an adversary, at least a significant competitor in the cyber domain.

At the *2024 NATO Summit* in Washington, DC, the allies decided to establish a new *Integrated Cyber Defense Center* at SHAPE to improve network protection and cyber deployment in various peace, crisis and conflict scenarios. NATO also encourages a unified approach in developing cyber defence capabilities by setting specific objectives for allied countries, supporting them to strengthen their national cyber defence by sharing information and best practices and organizing specialized exercises. This facility allows member states to voluntarily contribute to strengthening the cyber capabilities of other allies (NATO, 2024).

Over the last decade, NATO's cyber policies have also facilitated the development of links with the civilian institutions of the European Union, thereby strengthening civil-military partnerships. This dynamic takes place in a context where most EU member states are also NATO member states. Cyber defence is one of the areas of enhanced cooperation between NATO and the EU, as part of the two organizations' increasingly coordinated efforts to counter hybrid threats. NATO and the EU exchange information and best practices. Cooperation is also strengthened in training, research and exercises with tangible results in combating cyber threats. The North

Atlantic Alliance and the European Union cooperate on cyber defence through a technical agreement, which was signed in 2016. Given common challenges, NATO and the EU are strengthening their cooperation in the field of cyber defence, in particular in training and responses to cyber attacks.

CYBER THREATS FROM THE PEOPLE'S REPUBLIC OF CHINA AND IMPLICATIONS FOR NATO CYBER SECURITY

The rise of the People's Republic of China has fuelled competition between it and the USA, particularly in trade and technology. Even the USA has recognized the PRC as *"the only one country that has both the will and the ability to reshape the regional and international order"* (Zhang, 2024). The competition between the two superpowers is also taking place at a time when internet-based economies and cyber policymaking increasingly revolve around the three main models established by the USA, the PRC and the EU. Chinese cyber security policies remain at the centre of global debate and research (Jiang M., 2023). Cyberspace is an inherently insecure environment, so the cyber threats posed by the PRC to NATO security are multiple and complex, with significant implications for the security of the Alliance and its member states.

Thousands of cyber threats are reported worldwide every day, and many of them are attributed to the People's Republic of China. A recent study ranked the PRC as *"the most comprehensive cyber power"* after the USA, which is due to its prioritization of education in information science and technology and training of specialists for military cyber operations (Hlavek, 2021). As expected, the main country targeted by Chinese cyberspace operations is the USA, the most powerful NATO member state. Washington has also identified Beijing as the most significant espionage threat, with over $300 billion in annual losses from intellectual property theft (Kobzova, 2023). In addition, other NATO member states, particularly in Europe, have reported attacks originating from Chinese hackers. These attacks intensified when a number of European states banned PRC firms from participating in the development of 5G technology in their respective states (Reuters, 2023). Chinese IT companies, including Huawei, are receiving substantial government support, including subsidies and investment in research and development, which has propelled some of them, Huawei in particular, to the forefront of the global 5G technology industry alongside other well-known Western companies. The introduction of 5G technology by Chinese firms in global markets has met vehement opposition from some Western states, whose political leaders are

concerned about the security risks associated with Chinese technology and its potential to be used for espionage or disruptive purposes (The International Institute for Strategic Studies, 2021).

Moreover, in July 2023, new cyber operations were identified in NATO countries such as the UK, Slovakia, Czech Republic and Hungary (Sharwood, 2023). Frequent targets were diplomatic entities, foreign ministries, the private sector and various other institutions. A few months earlier, the European Union Agency for Cyber Security (ENISA) had issued a report exposing numerous cases of cyber espionage attacks on member states, including activities directed against German companies, Belgian ministries, French organizations, EU institutions and many others (ENISA, CERT-EU, 2023). On the other hand, the collection of data and other information about citizens or institutions of NATO member states through various media platforms further enhances Beijing's strategic advantage over its competitors. Along with its massive investments in emerging technologies and in educating specialists, Beijing has improved its techniques, tactics and effectiveness through the complexities of operating in the digital environment. The combination of all these elements have strengthened the PRC's leadership position by becoming one of the most important challenges facing NATO (Kobzova, ib.).

The overall objective of the threats targeted by the PRC is to gain political, military and economic advantage over Western nations. From a cyber security perspective, Beijing's strategic approach differs from that of other significant actors in this field, such as the Russian Federation, North Korea or Iran. The goal is not to compromise critical infrastructure, but rather, cyber espionage. Over time, Beijing has gained notoriety for its sustained cyber espionage activities in both industrial and military sectors. However, it is worth noting that, on occasion, Chinese hackers have also been involved in attacks aimed at disrupting critical infrastructure (Ib.).

Another aspect of the confrontation between the PRC and the USA is the geostrategic Asia-Pacific area of influence, where the two great powers have interests. One of the PRC's most recent and worrying cyber campaigns targeted the US island of Guam (Sanger, 2023). The cyber operation in Guam has highlighted the strategic role of this territory, given its geographic location close to Taiwan and the important military facilities it possesses, which are essential to the USA response capability in the event of an escalation of the conflict in the South China Sea. These cyberattacks, which targeted critical infrastructure such as military bases and transportation and telecommunications systems, indicate a significant departure

from conventional methods of cyber espionage, suggesting a dual purpose: reconnaissance and potential preparation for disruptive action. In support of this, a report published by New Zealand and Canada indicated that the Chinese malware was not solely intended for cyber espionage (Kobzova, ib.).

In its 2022 *Global Threat Report*, US-based cyber security company *Crowd Strike* ranked the PRC as a world leader in exploiting cyber vulnerabilities. The report emphasizes the advanced exploitation skills possessed by the Chinese hacker community, highlighting the significant technical development capability of the Chinese (US-China Economic and Security Review Commission, 2022). According to other public reports, over the past two decades, the PRC has been continuously engaged in offensive cyber operations. With the expansion of its economic and political ambitions, its influence in cyberspace has grown significantly. It is reflected by the growing number of state-sponsored non-state actors developing and deploying offensive cyber capabilities in support of national objectives, ranging from economic to national security (Handler, 2023). In response to all the activities in cyberspace involving NATO or its members, heads of state and government have taken some measures, either reactive or proactive, depending on the situation.

With the proliferation and sophistication of threats – including terrorism, cyber-attacks, disruptive technologies, climate change and challenges from Russia and the PRC to the international order –, NATO has adopted the *NATO 2030 Initiative*. This document aims to strengthen transatlantic cooperation and proactively address security challenges related to emerging and disruptive technologies, responding to the PRC's ambitions to dominate the artificial intelligence sector. Through this initiative, NATO is committed to investing in broadening and deepening strategic partnerships that reflect shared values and common interests, thereby strengthening transatlantic cooperation. Also, the PRC's activities in cyberspace are considered threats that require deep and rapid strategic adaptation on NATO's part to remain effective and relevant in protecting the security and prosperity of its members (NATO, 2021).

As a result, in order to effectively manage cyber incidents, NATO engages in continuous and coordinated preparedness. To this end, member states' representatives have agreed on the establishment of dedicated institutions capable of preventing, promptly responding to and rapidly remediating security problems in Alliance networks. These structures are essential for strengthening NATO's

resilience against cyber threats and maintaining operational stability in the face of modern challenges.

Operationally, the North Atlantic Alliance established a Cyberspace Operations Centre at Allied Command Operations (ACO) in Mons, Belgium in 2019. The main purpose of this centre is to monitor cyberspace and to coordinate and synchronize cyberspace operations with land, sea, and air operations (Brzozowski, 2018). This centre is essential for the Alliance's cyber security, as it can act as a deterrent and allows NATO to respond quickly and effectively to potential cyber attacks. The centre also enhances collaboration between member states and can form the basis for a NATO Cyber Command essential in the face of evolving cyber threats.

From a technical perspective, the NATO Communications and Informatics Agency (NCIA) interacts with the NATO Cyber Security Centre (NCSC) and the NATO Computer Incident Response Capability (NCIRC), and is responsible for developing, managing and securing the Alliance's cyber infrastructure. In addition, the NCIRC, through a dedicated coordination centre, enables member states to share information and techniques on cyber threats, including some indicators that may provide clues to the nature of the attacks. These NATO structures have contracts with leading IT defence companies on cyber protection services for the Alliance. Moreover, NATO's cyber rapid response teams are available for prompt deployment in support of Allies suffering cyber attacks (Marrone, Sabatino, 2021). This type of civil-military partnership strengthens cooperation and resilience in cyber security and defence.

It is widely recognized that the challenges in cyberspace are considerably different from those in other operational domains because it is an artificial domain, which is almost entirely man-made and controlled. In this context, the human resource is essential. As a result, adequate training of personnel becomes crucial for the prevention of cyber incidents or the effective management of existing ones. NATO invests strategically in the training of its specialists by organizing intensive courses at various academic institutions affiliated to the Alliance.

The PRC's cyber capabilities are a concern within the North Atlantic Alliance, which is why numerous countermeasures have been taken. In cyberspace, NATO should take a leading role in the international community in terms of legislation and legal regulation. Accordingly, the Alliance has established the Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn to strengthen cyber defence capabilities. This centre serves as the main hub for cyber research and strategic thinking facilitating not only advanced research but also the development

of innovative cyber defence strategies. It also emphasizes doctrine development, training and education to support interoperability and the exchange of best practices among NATO members and partners. The centre has developed a comprehensive guide to the rules and laws applicable to cyber warfare called the *Tallinn Manual* (Pfannenstiel, Cox, 2024). It is an academic document developed to provide a detailed interpretation of how existing international laws apply to cyber conflicts. This treaty would strengthen global security and allow NATO to more effectively defend against Chinese threats. At the same time, NATO specialists benefit from numerous training opportunities through participation in joint exercises and activities, organized by the Alliance or in cooperation with other partners. For example, in 2023, more than 3,000 participants from 38 countries – including NATO Allies and partners – took part in the annual *Locked Shields* exercise hosted by CCDCOE. This is the world's largest cyber defence exercise, which involved protecting information systems from real-time attacks and simulating tactical and strategic decisions in critical situations (NATO, 2023).

Such exercises are fundamental to enhancing cooperation and facilitating the exchange of best practices, playing a key role in strengthening ties between member nations. They create valuable opportunities for allies to test and improve common procedures in simulated situations, thereby increasing the effectiveness of responses in real crises. Moreover, these activities provide a new perspective on the importance of civil-military cooperation. By involving civilian entities, including universities and private sector research institutions, the exercises contribute not only to improving cyber defence capabilities, but also to enhancing synergies between civilian and military assets, a crucial factor in adapting to new technological challenges and managing complex cyber threats.

In an increasingly technology-dependent global context, such initiatives are vital for maintaining a strategic advantage in cyberspace. They not only strengthen the individual capabilities of each member state, but also provide a solid basis for effective collective defence. Exercises, together with other similar initiatives, also play a very important role in deterring adversaries, enabling the Alliance to respond promptly and cohesively to emerging threats and to protect critical infrastructure in member states. These activities enhance NATO's ability to effectively anticipate and counter potential attacks, thereby ensuring the security and stability of the region.

Another measure that NATO should apply would be to invest more in equipment, in the development of emerging technologies, in the specialization of personnel and in the development of cyber hygiene among the population,

so as to counter the disruptive effect of offensive actions targeting the Alliance's security. NATO can also remain competitive in the field of cyber defence and cyber security only through close cooperation with civilian, academic and private institutions, and it is through this civil-military synergy that the Alliance will be able to have a comprehensive response to cyber threats. Moreover, improving information sharing and collaborative practices between member states through the use of common platforms to share threat and vulnerability data in real time is key.

Last but not least, cyber diplomacy can set international norms and rules for behaviour in cyberspace, seeking to build a global agreement on prohibiting disruptive practices that could harm critical data, networks and infrastructure without remedy.

CONCLUSIONS

This study is not intended to be exhaustive research. Therefore, its approach is limited to specific aspects of cyber security without fully exploring all the associated geopolitical dimensions and multivalences. It represents a deliberate delimitation of the scope and breadth of the analysis, focusing on specific contributions of existing policy and scientific literature.

The limitations in this research consisted in the choice of only one alliance for the study, which allowed for a detailed focus, but also restricted the generalizability of the findings to other states or alliances. In addition, open-source materials on this topic are often contradictory, sketchy and unclear. This methodological decision was driven by the need for an in-depth analysis, which, despite its specificity, provides a solid basis for further extrapolations and comparative research in the field of cyber security. As a result, future research directions could include the analysis of cyber activities and their impact on cyber security, both at EU and international level. Therefore, for a proper understanding, cyber security requires a holistic perspective that integrates and analyses its multiple dimensions and the interactions between them.

The answer to the research question is not simple. Cyber security within an alliance must be assessed from a multi-layered and comprehensive perspective. So far, the People's Republic of China has not challenged the North Atlantic Alliance; however, its ambitions to dominate cyberspace loom as imminent challenges for NATO. In order to better manage cyber incidents, various measures have been proposed.

Finally, NATO must take a comprehensive approach to the PRC's cyber threats by investing in emerging technologies, strengthening cooperation with civilian and military partners, and educating cyber specialists. Also, through joint exercises and cyber diplomacy, NATO can contribute to the development of an international framework to promote responsible behaviour in cyberspace. The Alliance's response must be one based on prevention, deterrence and cooperation to preserve stability and security in an increasingly contested area.

BIBLIOGRAPHY:

1. Austin, G. (2018). *Cybersecurity in China the Next Wave.* Canberra: Springer.
2. Brzozowski, A. (17 October 2018). *NATO sees new cyber command centre by 2023 as Europe readies for cyber threats*.
3. Burke, E.J., Gunness, K., Cooper III, C.A., Coza, M. (2020). *People's Liberation Army Operational Concepts.* Santa Monica: RAND.
4. Chafetz, G. (31 July 2023). *How China's Political System Discourages Innovation and Encourages IP Theft.* SUA.
5. Denning, D.E. (2001). *Chapter Eight – Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*. In J. Arquilla, D. Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy* (pp. 239-288). RAND Corporation.
6. Diotte, P. (2020). *The Big Four and Cyber Espionage: How China, Russia, Iran and North Korea Spy Online*. In *Canadian Military Journal*, pp. 32-42.
7. ENISA, CERT-EU (2023). *JP-23-01 – Sustained activity by specific.*
8. Ford, C.A. (11 September 2019). *U.S. Department of States*, https://2017-2021.state.gov/: https://2017-2021.state.gov/huawei-and-its-siblings-the-chinese-tech-giants-national-security-and-foreign-policy-implications/, retrieved on 22 July 2024.
9. Grauman, B. (2012). *Cyber-Security: The Vexed Question of Global Rules.*
10. Hamilton, B.A. (2020). *Same Cloak, More Dagger: Decoding How the People's Republic of China Uses Cyberattacks,* https://www.boozallen.com/insights/cyber/chinas-cyberattack-strategy-explained.html#report, retrieved on 22 July 2024.
11. Hamilton, B.A. (2024). *How to succeed at annexation without really fighting – The PRC's Taiwan Cyber Strategy Explained.*
12. Handler, S. (31 January 2023). *The 5×5 – China's cyber operations*, https://www.atlanticcouncil.org/: https://www.atlanticcouncil.org/content-series/the-5x5/the-5x5-chinas-cyber-operations/, retrieved on 22 July 2024.
13. Hasanov, A.H., Iskandarov, K.I., Sadiyev, S.S. (2019). The Evolution of NATO's Cyber Security Policy and Future Prospects. In *Journal of Defense Resources Management,* vol. 10, no. 1(18), pp. 94-106.
14. Hlavek, A. (2021). *China cyber attacks: the current threat landscape.* Ironnet.
15. Hwang, J.-J. (2023). *Reframing China's Territory and Sovereignty in Cyberspace: Exploring Conceptual Territorialization and Claims of Cyber Sovereignty*. In *Issues & Studies A Social Science Quarterly on China, Taiwan and East Asian Affairs,* vol. 59, no. 4, 21.

16. Jiang, M. (2020). *Cybersecurity policies in China*. In L. Belli, *Cyber BRICS: Cybersecurity Regulations in BRICS Countries* (pp. 95-212). Berlin: Springer.
17. Jiang, M. (2023). *Chinese Cybersecurity Policies in the Age of Cyber Sovereignty*. In M. Timoteo, B. Verri, R. Nanni, *Quo Vadis, Sovereignty? New Conceptual and Regulatory Boundaries in the Age of Digital China* (pp. 77-90). Springer Nature Switzerland AG.
18. Jiang, T. (2019). *From Offensive Dominance to Deterrence: China's Evolving Strategic Thinking on Cyberwar*. In *Chinese Journal of International Review,* vol. 1, nr. 2, pp. 195-218, www.worldscientific.com., retrieved on 17 July 2024.
19. Jiang, T. (2022). *The Shift of China's Strategic Thinking on Cyberwarfare Since the 1990s*. In *Journal of Chinese Political Science*, pp. 127-149.
20. Jinghua, L. (22 March 2019), https://theglobalobservatory.org/2019/03/what-are-chinas-cyber-capabilities-intentions/, retrieved on 29 June 2024.
21. Jun, O. (2023). *Direction of Japan's New Cybersecurity Policy*. In *Asia-Pacific Review*, pp. 63-78.
22. Kobzova, L. (2023). *China's Cyber Threat: Implications for NATO and Potential Remedies.* Adapt Institute.
23. Marrone, A., Sabatino, E. (2021). *Cyber Defence in NATO Countries: Comparing Models.* Instituto Affari Internazionali.
24. NATO Strategic Concept (2010). *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization.* Lisbon: NATO.
25. NATO/North Atlantic Treaty Organization (2016). Warsaw Summit Communiqué. Warsaw.
26. NATO/North Atlantic Treaty Organization (2021). *NATO 2030.*
27. NATO/North Atlantic Treaty Organization (14 September 2023). *North Atlantic Treaty Organization*, https://www.nato.int/cps/en/natohq/topics_78170.htm, retrieved on 28 June 2024.
28. NATO/North Atlantic Treaty Organization (2023). Vilnius Summit Communiqué, https://www.nato.int/cps/en/natohq/official_texts_217320.htm, retrieved on 27 June 2024.
29. NATO/North Atlantic Treaty Organization (30 July 2024). *Cyber defence*, North Atlantic Treaty Organization: https://www.nato.int/cps/en/natohq/topics_78170.htm, retrieved on 29 June 2024.
30. Pfannenstiel, M., Cox, D. (2024). *NATO's Cyber Era (1999–2024) Implications for Multidomain Operations*. *Military Review Online Exclusive*.
31. Reuters (29 September 2023). *European countries who put curbs on Huawei 5G equipment*, https://www.reuters.com/: https://www.reuters.com/technology/european-countries-who-put-curbs-huawei-5g-equipment-2023-09-28/, retrieved on 29 June 2024.
32. Sanger, D.E. (24 May 2023), in Chinese Malware Hits Systems on Guam. Is Taiwan the Real Target?, https://www.nytimes.com/2023/05/24/us/politics/china-guam-malware-cyber-microsoft.html, retrieved on 29 June 2024.
33. Sharwood, S. (4 July 2023). *Undiplomatic Chinese threat actors attack embassies.*
34. Soesanto, S. (4 July 2022). *Cyber Deterrence Revisited*. Alabama: Air University Press.
35. The International Institute for Strategic Studies (2021). *Cyber Capabilities and National Power: A Net Assessment.*

36. The State Council Information Office of the People's Republic of China. (July 2019). *China's National Defense in the New Era*. Beijing, China: Foreign Languages Press Co. Ltd.
37. The White House (May 2011). International Strategy for Cyberspace – Prosperity, Security, and Openness in a Networked World. Washington.
38. Triolo, P., Sacks, S. (26 September 2017). *Center for Strategic and International Studies*, https://www.csis.org/analysis/shrinking-anonymity-chinese-cyberspace: https://www.csis.org, retrieved on 29 June 2024.
39. United Nations General Assembly (2011). *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General.*
40. U.S.-China Economic and Security Review Commission (2022), https://www.uscc.gov/sites/default/files/2022-11/Chapter_3_Section_2--Chinas_Cyber_Capabilities.pdf, retrieved on 29 June 2024.
41. Zhang, H. (12 July 2024). *What is the intention of NATO, the "war maker", to "directly warn" China?* China.

CYBER DEFENCE STRATEGIES IN THE HEALTHCARE SECTOR: DETERRENCE, RESILIENCE, AND CRITICAL INFRASTRUCTURE PROTECTION

Claudia LASCATEU, PhD

Cyber Security Superior Manager, Cyber Security National Directorate, Bucharest

Mihai CONSTANTINESCU, PhD Candidate

Cyber Security Superior Manager, Cyber Security National Directorate, Bucharest

DOI: 10.55535/RMT.2024.4.18

The integration of robust cybersecurity tools and technologies within healthcare institutions is a critical strategy for strengthening national security and enhancing deterrence, particularly within NATO framework. This article highlights the strategic importance in mitigating targeted cyber threats.

Critical tools for real-time threat detection, establishing secure network perimeters, and comprehensive network security are discussed for their efficacy in pre-empting and responding to sophisticated cyber-attacks. Additionally, the strategic outsourcing of cybersecurity services to specialized third-party providers is explored, demonstrating the enhanced defence mechanisms achieved through leveraging external expertise and advanced technologies.

The article underscores the necessity of a multi-faceted cybersecurity approach, analysing the strategy and policy applied to the unique demands of the healthcare sector. By enhancing the cybersecurity posture of healthcare institutions, this research posits a significant increase in national preparedness against targeted cyber threats.

Keywords: national security; cyber security; healthcare system; advanced technologies; NATO;

INTRODUCTION

Increasing reliance on digital technologies in critical sectors such as healthcare has brought to the fore the importance of robust cyber security as a pillar of national security. In an interconnected world, cyber threats targeting medical infrastructure have become a major concern, not only for public health systems, but also for national defence mechanisms. This growing vulnerability has required the integration of sophisticated cyber security measures aimed at reducing the risks associated with cyber attacks, especially those orchestrated by state and non-state actors.

This article aims to analyse the role of advanced cyber security solutions in strengthening national security in the health sector, with a particular focus on Romania's strategic approach, highlighted in the *Cyber Security Strategy* adopted by GD no. 1321/2021. In a broader geopolitical context, these measures align with NATO's defensive framework, which prioritizes infrastructure interoperability and resilience in the face of complex cyber threats.

The detailed exploration of technologies such as artificial intelligence (AI) for threat detection, endpoint protection and advanced data encryption demonstrate how these solutions not only ensure the confidentiality, integrity and availability of sensitive health data, but also contribute to threat deterrence. This is consistent with NATO's collective defence posture, which recognizes that disruption of critical health systems could have knock-on effects on national stability and international security. Moreover, through the lens of the Tallinn Manual 2.0 and International Humanitarian Law (IHL), the protection of medical infrastructures during cyber conflicts becomes a legal obligation, emphasizing the need for advanced defensive capabilities.

By adopting a multi-faceted approach to cyber security, Romania aims to strengthen its resilience in the face of increasingly sophisticated cyber threats, thus strengthening the security architecture not only at the national level, but also among NATO allies. This article highlights the imperative to combine technological innovation with strategic collaboration, both nationally and internationally, to protect healthcare infrastructures from sophisticated cyber attacks, thereby ensuring national security and public safety. Through an analysis of existing policies,

legal frameworks and advanced technologies, this study provides insights into the future of cyber defence in the healthcare sector as a central element in national and international security.

THE ROLE OF MEDICAL INFRASTRUCTURE IN NATIONAL SECURITY AND WITHIN NATO

The health system, through its accelerated digitization, has become an integral part of the national critical infrastructure, necessary to ensure public security and social stability. Within Romania's *Cyber Security Strategy*, protecting these infrastructures is essential for national security and defence against cyber attacks.

NATO recognizes the importance of critical infrastructures in maintaining national and regional stability. An attack on health systems not only affects the delivery of essential services, but creates vulnerabilities that can be exploited for political and military destabilization purposes.

The national cyber security system provides for the protection of the health sector by implementing specific measures, such as vulnerability assessment, incident prevention and rapid intervention in the event of cyber attacks.

Medical Infrastructure and National Security

The health system, through accelerated digitization, has become an integral part of the national critical infrastructure. The importance of medical infrastructure goes beyond public health, having a direct impact on national security and social stability. The protection of the medical infrastructure against cyber attacks is essential not only for the continuity of services, but also for preventing the exploitation of vulnerabilities by state or non-state actors, including in conflict situations.

According to Romania's *Cyber Security Strategy*, critical infrastructures, including the health sector, are essential for national security, requiring specialized cyber protection measures. In this context, compliance with International Humanitarian Law (IHL) and the Tallinn Manual 2.0 is crucial to addressing cyber attacks on critical infrastructure in a manner compatible with international law.

Protection of Medical Infrastructures within NATO and According to International Humanitarian Law

NATO recognizes the protection of critical infrastructures as essential to maintaining national and regional stability. Cyber-attacks on medical systems are considered a significant threat, having the potential to destabilize not only the provision of essential services, but also the political and military balance in a NATO member state.

According to Tallinn Manual 2.0, medical infrastructures are explicitly protected against cyber attacks in conflict situations. The manual states that attacks on medical IT systems are prohibited, as they are not legitimate military targets and are protected by the **principle of distinction**. Thus, the intentional destruction or disruption of medical services, whether by cyber or physical means, can be considered a violation of International Humanitarian Law.

Article 99 of the Tallinn Manual 2.0 emphasizes that medical facilities and other infrastructures providing care are protected from being legitimate targets in cyber armed conflicts, and states have an obligation to take appropriate measures to protect these targets against cyber attacks.

National Cyber Security System and Health Sector Protection

Romania, through the national cyber security system, implements concrete measures to protect critical infrastructures, including the health sector. These measures are aligned with international humanitarian law and the principles enunciated in the Tallinn Manual 2.0, which considers that medical infrastructures must be protected both in peacetime and during armed cyber conflicts.

According to Tallinn Manual 2.0, Romania must adopt preventive measures, such as:

- Assessing the cyber vulnerabilities of medical infrastructures and improving security to prevent large-scale cyber attacks.
- Preventing incidents by implementing advanced security solutions such as intrusion detection (IDS/IPS), data encryption and real-time system monitoring.
- Rapid intervention in case of cyber attacks by specialized teams, according to the provisions of IHL and Tallinn Manual 2.0, which emphasizes the need for a coordinated and proportionate response in the event of an attack.

Impact on National and Regional Security under International Humanitarian Law and Tallinn Manual 2.0

Cyber attacks on medical infrastructure can seriously disrupt the functioning of the health system, but also have a significant impact on the supply chain of the medical sector, which can cause serious consequences for national and regional security. In this context, IHL and Tallinn Manual 2.0 provide a solid framework for protecting not only medical infrastructures, but also systems associated with the cyber supply chain. In accordance with the **principle of proportionality** in the law of armed conflict, states must refrain from attacks that may cause disproportionate

damage to civilian infrastructure, including medical infrastructure. Tallinn Manual 2.0 reinforces these principles, highlighting that any attack on a hospital or medical IT system can constitute a serious violation of IHL.

The medical supply chain comprises a complex network of systems that include the production, storage and distribution of medicines, medical equipment and other critical materials required for the efficient operation of health services. In the digital age, this network relies heavily on IT infrastructures for order management, shipping and inventory monitoring. According to Tallinn Manual 2.0, a cyber attack on health infrastructure can severely affect the supply chain, with major side effects such as shortages of essential medical equipment or medicines for the population.

Article 70 of the Tallinn Manual 2.0 states that cyber attacks must be directed only at military targets and cannot include medical facilities or their associated IT systems. In addition, medical infrastructures must be **protected against indirect attacks or the collateral effects of cyber operations.**

Cyber attacks that disrupt the medical supply chain can have devastating consequences for the health system and national security. During the COVID-19 pandemic, we witnessed the vulnerabilities of supply chains, where any delay in the delivery of medical equipment or essential medicines had a direct impact on public health. In a cyber conflict, disrupting these chains can be used as a destabilizing tactic, leading to a health and social crisis of major proportions.

International Humanitarian Law provides for the protection not only of medical infrastructures, but also of the critical networks that support these infrastructures. Tallinn Manual 2.0 extends this protection to digital networks that manage the logistics and supply of medical resources, emphasizing that attacks on these networks are a violation of the IHL's Principle of Proportionality. A cyber attack affecting a hospital's supply chain, blocking the supply of essential equipment or medicine, could cause a disproportionate effect on the civilian population and could be considered a war crime.

NATO has recognized the **vulnerability of cyber supply chains** and established measures to protect critical infrastructures that support medical supply and logistics in the event of conflict. As part of cyber defence strategies, NATO promotes the sharing of information between member states to identify and prevent vulnerabilities in supply chains. In addition, NATO encourages collaboration between the public and private sectors to secure these critical networks.

Romania, as a NATO member, is obliged to adopt measures for the protection of the medical supply chain and the infrastructures that support the supply of essential

resources. In the context of a cyber threat, protecting these networks is essential to ensure the continuity of medical services and prevent a major public health crisis.

Under International Humanitarian Law and the provisions of the Tallinn Manual 2.0, states have an obligation to take proactive measures to protect critical infrastructures, including medical supply chains, against cyber-attacks (Article 99, the Tallinn Manual 2.0).

International Humanitarian Law and Tallinn Manual 2.0

Cyber attacks are recognized as modern forms of conflict and the Tallinn Manual 2.0 provides an essential legal framework for addressing them under the Law of Armed Conflict. Medical infrastructures, especially digitized ones, are protected not only by the traditional norms of IHL, but also by the new interpretations and guidelines provided by Tallinn Manual 2.0, which states that cyber attacks on medical infrastructures are prohibited, regardless of the form of the conflict.

*

Medical infrastructure is a critical pillar of national and international security, and its protection against cyber attacks is regulated by both International Humanitarian Law and the Tallinn Manual 2.0. These legal frameworks provide explicit protection to medical facilities, prohibiting any cyber attack that could disrupt their operation.

Romania, in collaboration with NATO and aligned with the provisions of Tallinn Manual 2.0, has the responsibility to implement proactive measures to protect medical infrastructures against cyber attacks. Cyber security measures and national strategies must be consistent with the provisions of IHL and Tallinn Manual 2.0 to ensure compliance with international obligations and protect these critical infrastructures during cyber conflicts.

CYBER THREATS AND THE NEED FOR AN INTEGRATED APPROACH

Romania, as part of a region increasingly exposed to large-scale cyber attacks, developed the *Cyber Security Strategy* in 2022 to protect critical infrastructures, such as the health sector, from cyber threats from state and non-state actors. This chapter analyses the need for an integrated approach to the protection of the health sector in the light of relevant international regulations and frameworks, including the NIS2 Directive, International Humanitarian Law, Tallinn Manual 2.0, Cyber Security Law no. 58/2023, and the measures included in the Inventory report.

Cyber Threats and the Relevance of the NIS2 Directive

The NIS2 Directive (Network and Information Security Directive), adopted at the level of the European Union, represents an essential legislative framework for the protection of critical infrastructures, including the health sector, against cyber threats. The directive focuses on the confidentiality, integrity and availability of data, aiming to improve the security and resilience of critical infrastructures at national and European level.

In the context of NIS2, the health sector is defined as an essential infrastructure, and Romania, as an EU member state, must implement robust cyber security measures to align with European requirements. They include:

- Regular security audits to assess cyber risks.
- Rapid response measures in case of cyber security incidents.
- Advanced cyber attack detection and prevention systems.

NIS2 requires the implementation of advanced technological solutions such as artificial intelligence and blockchain to ensure the security of medical data and critical health infrastructures.

Cyber Security Law no. 58/2023 and Its Application in the Health sector

Cyber security law no. 58/2023 provides a national legislative framework that aligns with the requirements of the NIS2 Directive and establishes clear obligations for the protection of critical infrastructures, including those in the health sector. This law introduces strict data protection and security incident management measures, requiring entities in the healthcare sector to implement technical and organizational security measures to prevent and promptly respond to cyber attacks.

Law no. 58/2023 requires:

- Mandatory reporting of cyber incidents affecting critical infrastructures, including healthcare IT systems.
- Sharing information between the public and private sectors to quickly identify and neutralize cyber threats.

This law joins other international regulations, such as the Tallinn Manual 2.0 and IHL, to ensure the protection of medical infrastructure against cyber attacks in accordance with international security standards.

The RO-CCH Report and the Implementation of Emerging Technologies

According to the Report *Inventory of cyber security tools and technologies suitable for or dedicated to healthcare and health institutions (D4.3)* from the Romanian Cyber Care Health Project – RO-CCH (RO-CCH, 2022), funded by the European

Commission through CNECT.H – Digital Society, Trust, and Cybersecurity, Romania has started to implement a series of advanced measures to strengthen the cyber defence capacity, with a focus on the protection of critical infrastructures in the field of health. The report highlights the importance of using emerging technologies such as:

- Artificial intelligence (AI) for real-time threat detection.
- Blockchain for securing medical data and supply chains.
- Advanced encryption to protect sensitive data from unauthorized interception.

These technologies are essential to respond to complex and evolving threats from state and non-state actors. Also, the mentioned RO-CCH report recommends regular audits and the use of incident management platforms to ensure the operational continuity of medical services in the face of potential cyber attacks.

The Need for an Integrated Approach

Romania, through the 2022 *Cyber Security Strategy*, is taking important steps in protecting critical infrastructures, but must continue to adopt effective measures in cooperation with its international partners, such as NATO and the European Union. Inter-agency collaboration and information sharing between the public and private sectors is crucial to creating a resilient cyber environment.

In addition, the integrated approach must also include measures to educate and raise awareness of medical and IT staff about new threats and technologies. Tallinn Manual 2.0, IHL, NIS2 and Law no. 58/2023 provide a solid framework for securing medical infrastructures, but the implementation of these regulations at national and local level is essential for the protection of the health sector against cyber threats.

*

Romania has developed a robust framework for the protection of critical infrastructures, including the health sector, through the 2022 *Cyber Security Strategy*, the NIS2 Directive, Law no. 58/2023, and the principles established in Tallinn Manual 2.0 and International Humanitarian Law. These measures are essential for ensuring the confidentiality, integrity and availability of medical data, but also for the protection of medical infrastructures against cyber attacks supported by state and non-state actors. Romania must continue to invest in advanced technologies, conduct regular security audits and strengthen international cooperation to create a resilient and secure cyber environment.

ADVANCED CYBER SECURITY MEASURES IN THE HEALTH SECTOR AND THEIR IMPACT ON NATIONAL SECURITY AND NATO STRATEGY

Romania's *Cyber Security Strategy*, provided for in GD no. 1321/2021 and adopted in 2022, promotes the use of innovative technologies, such as artificial intelligence and behavioural analysis systems, to improve detection and response capabilities in the health sector. According to GD no. 1321/2021, it is essential that health infrastructures should be protected by advanced technological measures, such as next-generation firewalls, continuous traffic monitoring systems and data loss prevention programmes. These measures are necessary to protect patient data and prevent cyber attacks that can destabilize the medical infrastructure.

Within NATO's strategy, interoperability and infrastructure security are key priorities. The use of these technologies in Romania contributes to strengthening cyber security in the field of health and to ensuring a robust cyber defence, compatible with NATO requirements.

National Policies and Strategies

Romania's *Cyber Security Strategy* constitutes the foundation of national policies in the protection of critical infrastructure, including the health sector. It promotes the use of innovative technologies to strengthen detection and response capabilities in the face of cyber threats, emphasizing the need to adopt advanced security solutions such as:

- Behavioural analytics systems, which help identify anomalous cyber activities and can detect attacks before they cause significant damage.

According to GD no. 1321/2021, health infrastructures are considered critical for national security, and their protection is essential to prevent cyber attacks that could destabilize the entire medical infrastructure. Technological measures promoted in this strategy include:

- New generation firewalls for network perimeter protection.
- Continuous traffic monitoring systems to detect suspicious activity.
- Data Loss Prevention (DLP) programmes, which protect sensitive patient data from theft or destruction.

These advanced measures help ensure the confidentiality, integrity and availability of patient data and represent an important barrier against cyber attacks aimed at destabilizing medical infrastructures.

Interoperability and NATO Strategies

Within the NATO strategy, cyber security of critical infrastructures, including the health sector, is considered a **collective security priority**. Romania, as a NATO

member state, aligns its national policies with the requirements of the alliance, ensuring interoperability and the ability to react unitedly to cyber attacks. NATO emphasizes the importance of interoperability between member states' cyber systems to ensure a rapid and effective response to coordinated attacks by state and non-state actors.

Among the technological and tactical measures promoted by NATO for the protection of medical infrastructures are:

- Incident management systems (IMSs), which integrate data from various sources and help detect and manage cyber incidents.
- Advanced end-point protection solutions to ensure the security of devices connected to the network.
- Data Loss Prevention (DLP) platforms, designed to prevent the leakage of sensitive data or unauthorized access to information critical to national security and public health.

These measures are essential to prevent attacks such as ransomware or other types of complex attacks that target not only medical data, but also the critical functioning of healthcare IT systems. Interoperability between these systems is crucial to ensure a robust cyber defence compatible with NATO standards, thus strengthening the collective defence of critical infrastructures in the region.

The Impact of Advanced Measures on National and International Security

The adoption of advanced cyber security measures in the healthcare sector has a profound impact on national and international security, contributing to the stability of critical infrastructures and defence against cyber attacks. This section analyses the implications of these measures from the perspective of cyber deterrence theory, compliance with international norms, and their role in strengthening national cyber defence capabilities, according to Romania's *Cyber Security Strategy*, Tallinn Manual 2.0 and International Humanitarian Law.

Impact on national security

Advanced cyber security measures have a direct impact on national security, particularly through the protection of critical healthcare infrastructure. According to cyber resilience theory, a nation's ability to withstand and rapidly respond to cyber threats ensures the continuity of essential services. Protecting IT systems that manage patient data and medical supply flows contributes to internal stability and the maintenance of public order, even in large-scale cyber-attack situations.

In accordance with Romania's *Cyber Security Strategy*, measures such as the use of artificial intelligence (AI) for incident detection and response, the implementation

of new generation firewalls and data loss prevention (DLP) systems, are key tools for preventing and managing cyber attacks on healthcare infrastructure. These technologies are essential to prevent the confidentiality, integrity and availability of medical data from being compromised and to protect the critical resources needed to operate healthcare systems.

According to the theory of proactive cyber defence, the use of technologies such as AI not only helps in real-time detection of threats, but also enables an early reaction to attacks, minimizing the impact on critical infrastructure. Implementing these measures helps ensure business continuity, a central national security objective in any cyber security crisis.

Impact on international security and NATO cooperation

At the international level, the integration of advanced security measures according to NATO standards contributes to the strengthening of collective security and compliance with the requirements of the cyber defence strategy of the alliance. Interoperability between national cyber systems and those of NATO allies is essential to ensure a robust and coordinated defence against cyber threats. According to collective security theory, the ability to respond quickly and effectively to cyber attacks helps deter state and non-state actors that may attempt to exploit vulnerabilities in medical infrastructures.

Technologies such as SIEM (Security Information and Event Management), advanced firewalls and end-point protection ensure the rapid detection and management of incidents, allowing Romania to act within NATO strategies and contribute to regional stability. The use of AI and behavioural analytics helps prevent sophisticated attacks and reduce response time, thereby strengthening cyber defence capability internationally.

The deterrent effect on malicious actors

Another key aspect of advanced cyber security measures is the deterrent effect they have on malicious actors. *Cyber deterrence theory*[1] suggests that the presence of advanced technologies, combined with the state's ability to detect and respond

[1] Deterrence theory can be examined in detail by distinguishing between two key concepts: denial deterrence and punitive deterrence. Denial deterrence involves preventing adversaries from achieving their goals by making attacks difficult or unlikely, typically through robust defensive measures such as advanced cybersecurity systems, encryption, and real-time threat detection. Punitive deterrence, in contrast, focuses on imposing significant consequences or retaliation on attackers, discouraging them from initiating attacks due to the high risks involved. In the field of cybersecurity, both strategies can be applied: denial through technical measures that make systems difficult to compromise, and punishment through legal and diplomatic measures. In the healthcare sector, punitive deterrence can take the form of legal and diplomatic responses to cyberattacks targeting healthcare infrastructure, including working with international allies to isolate malicious actors (A.N.)

quickly to attacks, creates a less favourable cyber environment for attackers. Romania, by adopting these measures, strengthens its deterrence capacity at the national and international level, making it difficult to compromise medical infrastructures.

Next-generation firewalls and DLP play a critical role in protecting healthcare infrastructures from the theft or compromise of sensitive data. According to the theory of denial deterrence, advanced cybersecurity measures increase costs and risks for attackers, thereby reducing the likelihood of successful attacks.

Protection of medical infrastructures according to Tallinn Manual 2.0 and International Humanitarian Law

In the context of Tallinn Manual 2.0 and International Humanitarian Law, advanced cyber security measures ensure legal protection of medical infrastructures in the event of cyber conflicts. The advanced cyber security measures implemented in Romania ensure compliance with these international norms, reducing the risks of violating the principle of distinction. By protecting medical infrastructures from cyber attacks, Romania fulfils its international obligations and contributes to maintaining global stability and security in the face of cyber conflicts.

The advanced cyber security measures implemented in the health sector, provided for in GD no. 1321/2021 and supported by the NATO strategy, have a significant impact on national and international security. The use of state-of-the-art technologies such as AI and advanced encryption, as well as the application of national and international policies and strategies, help strengthen the resilience of critical infrastructures and protect citizens against cyber attacks.

Aligning with NATO policies, adopting the measures of the NIS2 Directive and complying with the Tallinn Manual 2.0 norms ensure a robust and integrated protection of the health sector. These measures strengthen cyber defence at the national and international level, contributing to the stability and security of the region and the protection of critical infrastructures in the face of increasingly complex threats.

STRENGTHENING NATIONAL AND INTERNATIONAL SECURITY IN HEALTH SYSTEMS

Analysing the impact of cyber defence advanced measures on national and international security, we will highlight some of the theories applied in the health sector, such as: *"Defence in Depth", "Zero Trust", "Deterrence by Denial", "Cyber Resilience" and "Shared Responsibility".*

The mentioned theories underline the need for an integrated framework, which should include advanced technological measures, institutional cooperation and international partnerships, to ensure the effective protection of critical infrastructures. By implementing these theoretical frameworks, Romania could contribute to strengthening the national and regional security, in compliance with international norms as well as with NATO and EU standards in cyber security.

"Defence in Depth" Theory and Its Application in the Health Sector

"Defence in Depth" theory is a key concept in cyber security and promotes the idea that effective security is based on multiple layers of defence. In the context of healthcare cyber security, this approach is applied by using a combination of technologies, procedures and organizational measures to protect critical infrastructure.

Advanced technological measures such as next-generation firewalls, data encryption and end-point protection are only one layer of this multi-level system. The implementation of data loss prevention (DLP) systems, SIEM platforms and behavioural detection solutions constitute other layers of defence, creating a resilient barrier against cyber attacks.

This theory holds that reducing reliance on a single protection mechanism and creating a multi-layered security architecture help delay and detect cyber-attacks, thereby reducing their success-associated risks. In the healthcare sector, the application of the *"Defence in Depth"* theory contributes to the protection in depth of sensitive data and critical functionalities, increasing the degree of system resilience.

"Zero Trust" Theory and the Protection of Medical Data

"Zero Trust" theory has become a central paradigm in modern cyber security. It implies that there should be no implicit trust between different network segments or between users accessing the resources. In a *"Zero Trust"* system, access to resources is only granted based on continuous checks of identity and compliance with security policies.

In the health sector, this theory is applied by strictly controlling access to medical data and essential infrastructures. Every access is monitored and verified, eliminating the risk of an attacker gaining unauthorized access and stealing or compromising critical data. Data encryption and the use of multi-factor authentication (MFA) are central to the implementation of this theory.

Adopting the *"Zero Trust"* model in healthcare infrastructures helps create a more secure cyber environment and significantly reduces the risk of internal

or external attacks that could compromise patient data. In an international context, this model is essential to ensure interoperability and protection of sensitive data between NATO and EU partners.

"Deterrence by Denial" Theory and Cyber Deterrence

"Deterrence by Denial" theory is an approach that focuses on preventing the success of an attack through technical and organizational measures that make attacks extremely difficult to carry out. In the case of the health sector, the application of this theory consists in the development of resilient cyber systems, so that attackers can be deterred from the start, due to the complexity and effectiveness of the security measures implemented.

Advanced cybersecurity measures such as real-time anomaly detection, continuous monitoring, and the use of automated cyber incident response solutions are all tools that contribute to *deterrence by denial*. A clear example is the deployment of AI technologies for behavioural analysis that can proactively detect and respond to attacks before they become a major threat.

In this context, the state's ability to prevent the success of cyber attacks on health infrastructures creates a deterrent shield that protects both national and international security. This theory also aligns with the *Active Defence Theory*, which involves continuous monitoring and intervention to prevent malicious activities.

"Cyber Resilience Theory" and the Importance of Recovery Capabilities

"Cyber Resilience" theory is central to understanding the impact of advanced cyber security measures on national and international security. Cyber resilience refers to the ability of a critical infrastructure to detect, withstand and quickly recover from a cyber attack, ensuring the continuity of essential operations.

In the healthcare sector, it means that not only prevention and detection measures are important, but also the ability of systems to return to a normal operational state after a cyber incident. Implementing disaster recovery plans (DRPs) and backup systems is central to this theory, complementing advanced cyber security strategies.

Resilience capabilities are critical in international collaboration, as cyber attacks can simultaneously affect infrastructure in multiple countries. Romania's ability to collaborate effectively with its NATO and EU partners to ensure the operational continuity of health infrastructures is a central pillar in its cyber security strategy.

"Shared Responsibility" Theory and the Collaboration between the State and the Private Sector

Another relevant theoretical framework for analysing the impact of advanced cyber security measures is the *"Shared Responsibility"* theory. It suggests that the cyber security of critical infrastructures such as the health sector cannot be ensured by the state alone, but requires close collaboration between the public and private sectors.

In this context, the state creates the legislative framework and the basic infrastructure for cybersecurity, but private entities – such as healthcare providers and technology companies – play a crucial role in implementing and maintaining security measures. This partnership between the state and the private sector is essential to ensure the continuity and resilience of the medical infrastructure against cyber threats.

Law no. 58/2023 imposes this principle by requiring entities that operate critical infrastructures to collaborate with national authorities to protect their systems, in accordance with international requirements.

CONCLUSIONS

As cyber attacks become more sophisticated and frequent, future research directions in cyber security for critical infrastructures, including the healthcare sector, should explore several key areas to support the continued evolution of protection and defence measures.

By implementing Romania's *Cyber Security Strategy* and adopting a position consistent with NATO standards and the requirements of the NIS2 Directive, Romania is strengthening its cyber defence capabilities. These measures not only protect critical health infrastructures against cyber attacks, but also create a significant deterrent effect on state and non-state actors who would attempt to exploit digital vulnerabilities.

At the same time, the application of the principles of International Humanitarian Law and the norms of Tallinn Manual 2.0 underlines the need to protect medical infrastructures in the context of cyber conflicts, ensuring Romania's compliance with international legislation on the protection of civilians and essential infrastructures. This legal framework provides a solid basis for the protection of critical health infrastructures and contributes to maintaining national and regional stability.

In conclusion, we consider that advanced cyber security in the health sector is an indispensable component of national and international security, and the application of innovative technologies, along with compliance with international

norms, is an effective strategy for protection against cyber threats. By collaborating with international partners and implementing robust security measures, Romania strengthens its leadership position in regional cyber security and contributes to the collective resilience of NATO and the European Union. This holistic approach ensures the protection of citizens and critical infrastructure in the face of the complex challenges of modern cyberspace.

BIBLIOGRAPHY:

1. *International Humanitarian Law and Civil Infrastructure Protection,* https://www.icrc.org/en/document, retrieved on 12 June 2024.
2. *EU Cyber Resilience Act*, https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:52022PC0454, retrieved on 23 May 2024.
3. Hotărârea de Guvern/Government Decision no. 1.321 on 30 December 2021, to adopt *Strategia de securitate cibernetică a României pentru perioada 2022-2027/ Romania's Cyber Security Strategy* and its implementation plan, https://legislatie.just.ro/Public/DetaliiDocumentAfis/250128, retrieved on 13 August 2024.
4. *Inventory of cyber security tools and technologies suitable for or dedicated to healthcare and health institutions (D4.3) "Romanian Cyber Care Health – RO-CCH"*, RO-CCH - DIGITAL-2022-CYBER-02, https://dnsc.ro/pagini/proiect-ro-cch, retrieved on 22 May 2024.
5. *Legea nr. 58/2023 privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative/Law no. 58/2023 regarding cyber security and defence*, https://legislatie.just.ro/Public/DetaliiDocument/265677, retrieved on 2 June 2024.
6. *NATO's Concept for Deterrence and Defence*, https://www.nato.int/docu/review/articles/2021, retrieved on 22 may 2024.
7. *NATO Cyber Defence Policy*, https://www.nato.int/cps/en/natolive/topics_78170.htm., retrieved on 22 June 2024.
8. RO-CCH (2022), https://dnsc.ro/pagini/proiect-ro-cch, retrieved on 14 June 2024.
9. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, https://ccdcoe.org/research/tallinn-manual, retrieved on 23 May 2024.

NATIONAL DOCTRINE AND STRATEGY – BASIS FOR THE NATION'S SUCCESS –

Major General (ret.) Associate Professor Grudi ANGELOV, PhD

National Security Department, Faculty of Information Technologies, University of Library Studies and Information Technologies, Sofia

DOI: 10.55535/RMT.2024.4.19

This article sheds light on the importance of both national doctrine and national (grand) strategy for increasing the national power of the state, and their significant role for the development of the country. It depicts the importance of setting up the national ideal, national interests and goals, as well as the accomplishment of the planned task with the dedicated means. National identity, national unity and participation in organizations such as EU and NATO are important for the development of the country's strategic agenda.

The national doctrine and strategy are long-term documents, enabling the society to have a good foundation for developing its strategic documents concerning the governance of the state and ensuring the prosperity of the nation. On the other hand, both strategic documents also have their restraining effect regarding the deterrence of desires for a sharp change of strategic interests and objectives of the nation.

Keywords: national; strategy; doctrine; interests; goals;

INTRODUCTION

Since 1989, the Bulgarian society has been looking for determining its national identity. Bulgarian politicians, despite leading the nation toward prosperity and democracy, have been arguing with each other to achieve their political goals. Throughout this period, we have witnessed political conversations that are not based on the consensus in favour of the individual citizen of this society. Furthermore, the citizens have witnessed the use of hate language leading to the disunity of the nation. All these years of wandering in search of democratic values, copying different models of the state's behaviour and experimenting with different political projects in search of the *"messiah"* who would lead the country out of the constant crisis (mostly political) in which it is fallen, we dare not look at ourselves.

In years of crises, pandemics and a war that has led to a crisis of global proportions, it is more than ever necessary to turn to the roots of our history to draw knowledge, wisdom and learn the lessons we need for the progress of the nation. It is also necessary to analyse the doctrines and strategies, especially grand strategies, of our neighbours, allies and partners, as well as the changes taking place in Europe and the world. It is necessary to get into the essence of their national policies and the means they use to achieve their national interests. A large number of these countries owe their success and prosperity to the consistent pursuit, achievement and defence of their national interests as enshrined in their national doctrines.

On the other hand, since the beginning of the 21st century, we have witnessed a number of conflicts, the latest of which is on the territory of Europe. The reasons for the emergence of these conflicts and the subsequent armed clashes (wars) bring us back to Clausewitz's definition that *"war is simply a continuation of political relations with the addition of other means."* (Clausewitz, 1976, p. 605). Later in the same chapter, Clausewitz goes on to note that *"we deliberately use the phrase ‹with the addition of other means› because we also want to make it clear that war does not in itself stop political communication or change it into something entirely different."* (Ib.). The conclusion that can be drawn from these two quotes is that wars arise as a result of the pursuit of political goals framed in a strategy where national interests are clearly formulated, national goals are defined and the state's resources are determined to achieve them.

Historically, national power has generally been associated with the presence of military capabilities. In general, power has various functions, the main of which being the provision of conditions for achieving the goals and interests of the individuals and groups of people. One of the most important functions of the national power of each individual state is the achievement (satisfaction) of national interests, their maintenance and expansion.

National goals and interests are also active and constantly changing. National power and security can also be related to national goals. Therefore, it can be said that power is both an end and a means of achieving national interests. The objective form and the main manifestation of the application of national power is represented by the national doctrine or national (grand) strategy.

When considering any national doctrine, one must note the fact that *"the creation and affirmation of national doctrine as an official document presuppose national consent."* (Velev, 1997, p. 7). When emphasizing the need for national agreement, the following aspects are taken into account: the achievement of a unified understanding of all the political parties represented in parliament regarding the definition of the national ideal, national interests (mod.bg, 2018) (listed in the updated National Security Strategy) and goals, the ways for their realization, and also the means for their achievement. The doctrine, on the other hand, sets a kind of framework for the political subjects, in order to avoid future drastic changes in the already accepted and established ways of the state development. The doctrine and national strategy are to be established to overcome the excessive politicization of society and to direct its energy solely to the prosperity of the individual citizen of the state and the well-being of the nation.

In the chapter *"National interests, goals and priorities"*, Valeri Rachev and Georgi Bakhchevanov compare national interests with those of an individual, writing that *"Nations, like individuals, have certain interests based on their internal values, recognized goals, means and motivating actions."* (Rachev, 2005, p. 64).

CORE OF NATIONAL DOCTRINE AND NATIONAL (GRAND) STRATEGY

The concept of *"national doctrine"* has failed to establish itself over the years in Bulgarian society, and instead of developing and adopting a national doctrine, which defines the national ideal and provokes the unity and development of the nation, Bulgaria's political elite has avoided talks on the development of a national doctrine and prefers to develop and adopt a National Security Strategy, in 2011, which was later updated in 2018 and the term of operation was set until 2025.

The situation regarding the so-called *"Grand Strategy"* or national strategy that could replace the national doctrine to some extent is the same. There is a lack of will amongst politicians, for such a strategy to be developed and endorsed by the politicians. There are more than two hundred and forty-seven strategic documents issued by the Bulgarian Parliament and Ministerial Council just to meet current requirements of the political situation.

In 1997, a few years after the change of the totalitarian regime of the Bulgarian Communist Party, a group of Bulgarian scientists and intellectuals developed a national doctrine: *Bulgaria in the twenty-first century, Bulgarian National Doctrine* (Velev, 1997). It did not reach acceptance by parliament regardless of the fact that for the first time a conceptualization of basic concepts such as doctrine, ethnicity, nationality, nation etc. was made.

When the question of national doctrine is raised, it is necessary to delve into the semantics of the words or what they represent. In the *"Bulgarian National Doctrine"* (Ib.) it is written that the national doctrine represents a theoretically grounded system of officially accepted views and principles about the historical aspirations, perspectives and goals of the nation, which point the way to the realization of the national ideal (Ib.). Furthermore, the implementation of such a doctrine through developed and adopted programmes (strategies and policies) makes it possible to determine the behaviour of the institutions in forming the internal and external policies of the state for a long period. It is clear from the definition that the national doctrine focuses mainly on the development and functioning of the state over a considerably long period comprising at least fifty years, why not more. Examples in this regard are our neighbours: Greece, Serbia and Türkiye with their doctrines. The Greek national doctrine *"Megali Idea"* (Great Idea) was developed more than one hundred and ninety years ago. *"The Blueprint"* – the Serbian National Doctrine was created in 1844 and subsequently updated in 1985. The doctrine was developed by the Serbian Academy of Sciences and was announced as a *"Memorandum"* issued by the academy. As far as Türkiye is concerned, its national doctrine – *"Peace in the Country, Peace with the World"* was announced by Kemal Atatürk in 1925 and it is currently being updated based on the rapidly changing security environment and changes in Türkiye's political life in recent years.

The national doctrine lays the foundations for the preservation and development of the nation, on the one hand, and creates confidence in the future of the nation, on the other hand. This confidence in the future can be achieved by:

- Precise and clear formulation of a national ideal, uniting all strata of the nation regardless of race, gender, ethnicity, education, culture, social status etc. The same should unite the nation and lead to its unity;

- Determination of adequate national interests, which should not be divided into *"vitally important and other national interests"*, but should determine the behaviour of the entire nation and not allow for their interpretation in order to extract short-term political dividends;
- Formulation of national goals and determination of ways to achieve them in the long term;
- Development of policies and programmes to fulfil the set goals;
- Determining the means (resources) to achieve the goals in pursuit of national interests;
- Assessment of available resources and their prioritization for the fulfilment of national goals and interests.

Reviewing the essence and content of the national doctrine, the question should be asked: *How does the doctrine differ from the strategy?*

Strategy (from Greek: στρατηγία, stratēgia, *"art of military leadership, office of military commander, command etc."*) is a high-level plan to achieve one or more goals under specific conditions of uncertainty. It is important because resources to achieve these goals are usually limited. Strategy usually involves setting goals, determining actions to achieve the goals, and mobilizing resources to accomplish those goals. The strategy describes how to achieve the final goals through the available means (resources), as the organizational studies management is usually charged with the task of defining the strategy, and the strategy itself can arise as a template/model of activity. Strategy includes activities such as strategic planning and strategic thinking.

According to a joint publication of the US Joint Chiefs of Staff, strategy is the art and science of developing and using the instruments of national power in a synchronized and integrated manner to achieve national and/or multinational objectives (Department of Defense Dictionary of Military and Associated Terms, 2004, p. 509).

Both definitions are relatively correct, but none of them gives a clear and complete picture of the role and complexity of strategic thought at high levels of government. At these levels, strategy is the art and science of developing and using a state's political, economic, socio-psychological and military capabilities in accordance with political directives to produce effects that protect or advance national interests in relation to other states, non-state actors, or circumstances.

The strategy itself is neither simple nor easy to understand. The very word *"strategy"* has become a cliché in our daily lives. It is present both in every conversation that two people have on the street and in the news broadcasts. We tend to use the word *"strategy"* as a general term for a plan, concept, course of action,

or vision for a direction to proceed at a personal, organizational, and governmental level. Moreover, it does not give a clear idea and does not describe when and under what conditions the strategy development process is initiated, on what basis the analyses are made regarding the security environment and the effects they have on the determination of national interests, policies, national goals, paths, and the means to achieve them.

Generally speaking, strategy at all levels is a set of goals, concepts and resources within acceptable limits of risk to create more favourable conditions and/or results that would otherwise exist by chance or could be exploited by a third party. One of the definitions states that *"strategy"* is the art and science of developing and using the instruments of national power to synchronize and integrate ways to achieve national and multinational goals. Both definitions are useful, but neither fully captures the role and complexity of strategic thought at the highest levels of state. Strategy seeks synergy and symmetry of goals, concepts and resources, to increase the possibility of success of government policies and to increase the effects of that success.

The strategy also provides a coherent plan to bridge the gap between today and the desired future. In the context of the state, strategy is the use of specific instruments of power (political, diplomatic, economic, military and information) to achieve the political goals in cooperation or in competition with other actors pursuing their own – possibly conflicting – goals. In other words, strategy is the application of the state power, with its inherent natural and public resources, to achieve political goals in an emerging, dynamic and competitive strategic environment.

The basic assumption of national perspective strategy is that all nation-states and non-governmental organizations have interests, which they pursue in the best ways for them. Interests represent a desired end state, categorized in terms such as survival, economic well-being, a favourable world order, and enduring national or group values. Interests are drawn from these broad categories as reflected in the strategic environment and can be defined more specifically in the context of the issues at hand. The elements of national power are the resources used to promote or advance national interests.

When we talk about strategy, we can say that, in general, it is defined by the art of the political leaders of a country to consider the capabilities, opportunities and level of national power, on the one hand, and the achievement of its national interests and goals, on the other hand. As a next step, they must define and adopt policies to achieve national goals and interests using the level of national power achieved.

Based upon the scientific books in economics: *"strategy is a long term (five-year) plan for development"* (Tanev, 2016, p. 8). Contrary to economic science books, political strategies meanwhile are developed for a period of at 20-30 years. On the other hand, they are *"dedicated to taking and keeping the power"* (Ib.) National strategies entail even much longer periods, being focused on: the direction for the country to develop its economy, education etc. In the long term, national strategy means that it has to cover a period ahead between 50 and 70 or 100 years. Therefore, there is a need for the national strategists' mindset to change. The strategy is to form the thinking today, in the vision of the achievements.

However, when it comes to developing a national strategy, it is absolutely and uncompromisingly necessary to analyse the security environment and clearly assess and define the risks and threats to the country's security, and subsequently to formulate national interests and goals.

Comparing the definitions of doctrine and strategy, it is evident that the strategy contains some of the attributes of the doctrine such as goals, determining ways to achieve these goals and resources, but in a defined period with a short time horizon. On the other hand, strategies are the ways and the means to fulfil national interests and goals. An example in this regard is the *"Updated National Security Strategy"* adopted in 2018. The national ideal of the Republic of Bulgaria is not defined in the strategy, and the national interests are divided into *"vital interests"* (mod.bg, 2018) and *"other important interests* (ib.). National objectives are limited, committed to the national security protection system and correspond to sectoral policies relating to the security of the state etc.

THE NATIONAL DOCTRINE AND THE FUNCTIONING OF THE STATE

What is the national doctrine? Why is the national doctrine the basis (foundation) for the functioning of the state?

To answer these questions, it is necessary to look at the doctrine through the lens of time and realize that it *"reflects the experience, maturity and purposefulness of the nation"* (Velev, ib). National doctrine makes the connection between generations, preserving the history, experience and knowledge of generations; it analyses current events and plans the nation's future. The national doctrine determines the behaviour of the state and its institutions in the formulation and implementation of the country's internal and external policy for a long period.

On the other hand, the main objectives of the national doctrine are:

- Assisting Bulgarian politicians and public officials in the implementation of the Bulgarian national ideal (after its formulation) and the protection of national interests;

- Mobilization of the nation's energy and will for the development of national unity for the achievement of the national ideal;
- Ensuring primacy in deciding and protecting national interests regardless of the changes in the political life of the state and the goals of individual political parties and movements;
- Serving the Bulgarian national ideal and Bulgarian national interests.

The national doctrine includes the national ideal, national interests and national programmes (policies) to meet them. Moreover, it is subject to updating to meet the challenges of the changing security environment.

As mentioned above, the national ideal is one of the basic attributes of the doctrine and represents the ultimate goal of the nation. It is a dynamic category referring to specific historical goals and objectives. It arises at a given stage of the nation's development to serve certain geopolitical, ethno-demographic, cultural, economic and other interests. The national ideal is the basis for determining national interests, and therefore for the formation and development of national policy.

National interests are other important parts of national doctrine. They are the main driving force of the nation and the state, being the basis of the implemented state policy. Over the years, in different historical periods, Bulgarian national interests have often been clearly formulated and adequately planned, leading to the rise of the Bulgarian state and statehood. Examples in this regard are:

- Conversion of the Bulgarians;
- Expansion of Bulgaria's borders under Khan Krum, Khan Omurtag, Tsar Simeon, Tsar Kaloyan and Tsar Ivan Asen II;
- Achievement of national aspirations for an independent church and own state.

On the other hand, there have been moments when the national interests were unrealistic, incorrectly defined, entailing excessively high expectations, which led to the cessation of the existence of the Bulgarian state for long periods. Examples of the kind are:

- The fall of the Bulgarian state under the Byzantine and Ottoman slavery, respectively;
- The wars in which the Kingdom of Bulgaria participated – Inter-Allied, World War I and World War II;
- Acceptance of the dominance of the *"great powers"* as a result of the decisions of the Berlin Congress and the Paris Treaties of 1919 and 1947;
- The long-term subordination of the Bulgarian internal and external policies of the state to the Comintern and the USSR.

Today, we are witnessing an inadequate use of the term national interest by Bulgarian public officials and police without a clear understanding of its content. National interests *"represent the collective need of the nation and are an expression of historically necessary and justified rights and actions"* (Velev, p. 37), therefore cannot, and should not be used for political PR and lobbying. The examples in the past two years in the political life of Bulgaria are extremely numerous. A large number of politicians use *"national interests"* as a means of dealing with their opponents or in their election campaigns without even knowing exactly where they are defined and who they are.

From everything presented so far, it is necessary to conclude that the national ideal and national interests are in a continuous symbiosis and interaction. National interests derive from and are a consequence of the national ideal as they reflect the various manifestations of the national ideal (political, cultural, economic, geopolitical, ethno-demographic etc.).

The processes that create them shape strategies. If designed well, the strategy formulation process allows decision-makers to assess the political, security and budgetary environment, identify opportunities for a country, weigh risks, possible solutions and trade-offs that need to be made and determine the best way to address the challenges of the changed security environment. It is possible to develop a good strategy from a not particularly good process and vice versa. A good strategy development model can lead to a bad strategy.

On the other hand, the doctrines require a precise analysis of the geopolitical environment and a precise assessment of the future geopolitical processes, which will enable a precise determination of national interests, strategic (national) goals and tasks. Using the analysis, assessment and impact of changes in the security environment, the means to achieve these goals and interests will be determined.

By their nature, national interests could be divided into long-term (for a period of at least fifty years) and short-term (for a short period, requiring their rapid achievement).

CONCLUSIONS

Taking into account everything mentioned above, it could be concluded that the development of national doctrine and/or strategy is a complex and challenging process. The complication stems from the fact that in the process of their development it is necessary to involve a large number of scientists and experts from practice, who possess different knowledge, experience and interests. Moreover, the difficulty is also determined by the need to present the doctrine or strategy in a convincing way to the political forces and the public.

On the other hand, the result of the efforts of a team with different interests is the presentation of a science-based document that presents the national doctrine and strategy as well as the reasons that necessitate their development. When developing these strategic documents, it is necessary to consider the basic concepts and principles that form the system of views for determining the national ideal and the national interests of the nation, as well as the means for their achievement.

Both national doctrine and national strategy are phenomena that can be observed in defining and meeting national interests, therefore representing essential factors in the development of the modern state. They provide an opportunity to overcome political extremes and confrontations between different parties and governments, thus generating continuity in achieving national interests and goals. The national doctrine is a long-term document that will enable continuity and consistency in fulfilling national interests. Therefore, an opportunity will be given for the normal functioning of the state and the development of statehood.

Finally, yet importantly, a vital element of the creation of strategies is the achievement of agreement on its content – agreement between institutions, between rulers and ruled, between politicians and experts, between national and international institutions, between present and future generations.

Acknowledgement and financing:

This work was supported by the NSP SD program, which has received funding from the Ministry of Education and Science of the Republic of Bulgaria under the grant agreement no. Д01-74/19.05.2022.

BIBLIOGRAPHY:

1. Clausewitz, von, C. (1976). *On War.* New Jersey: Princeton University Press.
2. Department of Defense Dictionary of Military and Associated Terms. (2004). *Joint Staff, J-7, Joint publication 1-02.* Washington D.C. The USA.
3. mod.bg. (2018). *Aktualizirana strategiaza nacionalna sigurnost.* Изтеглено на Aug 2023 г. от www.mod.bg: https://mod.bg/bg/doc/cooperation/20181005_Akt_strateg_NS_RB.pdf, retrieved on 5 September 2024.
4. Rachev, V., (2005). *Национални Интереси и приоритети, Национална и Международна сигурност.* Sofia, Bulgaria: Voenno izdatelstvo.
5. Prof. Velev, G. (1997). *Bulgaria prez dvadeset i parvi vek, Balagrska natsionalna doktrina, Parva chast, Fundament na Balgarskata natsionalna doktrina.* Sofia: Znanie EOOD, ISBN 954-621-113-3.
6. Tanev, T. (2016). *Kak mislqt stratezite*. Bulgarian Academy of Science *"Prof. Marin Drinov"*, ISBN 978-954-322-862-1.

THE MINES WAR IN THE BLACK SEA: AN UNFINISHED CONFLICT

Navy Captain (ret.) Associate Professor Romeo BOȘNEAGU, PhD
"Mircea cel Bătrân" Naval Academy, Constanţa
DOI: 10.55535/RMT.2024.4.20

Mine warfare has become an important aspect of the ongoing conflict between Russia and Ukraine in the Black Sea. The strategic use of naval mines represents a threat to both military and civilian ships, affecting naval and maritime security, as well as strategic stability in the Black Sea basin. The paper examines the types of mines used in this conflict, the number and locations of mines discovered in the Black Sea in the last two years, the entities involved in demining operations, and the types of vessels used in these efforts. It also addresses the future of mine warfare in the Black Sea – a region of significant geopolitical importance, serving as a strategic maritime gateway linking Eastern Europe, the Caucasus and the Middle East to the rest of the world. In recent years, the region has seen an increase in military tensions as the ongoing conflict between Russia and Ukraine has extended to the sea, transforming parts of the Black Sea into a dangerous area for navigation and shipping because of the use of mines.

Keywords: naval mine; Black Sea; security; Ukraine; Russia;

INTRODUCTION

The Black Sea has long been a region of significant geopolitical importance, serving as a strategic maritime gateway connecting Eastern Europe, the Caucasus, and the Middle East to the rest of the world. In recent years, the region has witnessed increasing military tensions, with the ongoing conflict between Russia and Ukraine playing a central role. One particularly concerning aspect of this conflict is the use of naval mines, turning parts of the Black Sea into a hazardous area for military and civilian shipping alike. This *"Mines War"* is emblematic of the evolving nature of naval warfare, where traditional methods blend with modern technology to create new forms of conflict at sea.

Naval mines have played a crucial role in the ongoing conflict between Russia and Ukraine in the Black Sea. As Ukraine has sought to defend its coastline and strategic maritime assets, it has deployed various types of mines to deter and disrupt Russian naval operations. However, the deployment of these mines has led to unintended consequences, with some mines drifting into the territorial waters of neighbouring countries like Romania, Bulgaria, and Türkiye. This paper explores the types and characteristics of Ukrainian mines used in the conflict, the reasons these mines have drifted from Ukrainian waters to those of other Black Sea states, and the broader implications of this phenomenon.

Naval mines have been used for centuries as a cost-effective and efficient means of controlling sea lanes, denying enemy access, and inflicting damage on opposing fleets. The Black Sea, historically, has seen several instances of mine warfare, most notably during the Crimean War (1853-1856), the First World War, and the Second World War. However, the modern iteration of the Black Sea mines war is being driven by recent geopolitical changes, from 2022 onwards, namely the naval war between Russia and Ukraine.

THE USE OF MINES IN THE BLACK SEA CONFLICT

Naval mines in the current Black Sea conflict serve multiple strategic purposes. They are deployed by both Russian and Ukrainian forces to achieve several objectives:

❖ **Area Denial and Coastal Defence**: Mines have been used to create exclusion zones, preventing enemy ships from approaching sensitive coastal areas, ports,

and naval bases. For instance, Ukraine has reportedly deployed mines near its ports in Odessa and Mykolaiv to prevent a potential Russian amphibious assault. Similarly, Russia has used mines to protect its naval installations in Crimea and deter Western naval support for Ukraine.

❖ **Economic Disruption**: Mines pose a significant threat to commercial shipping, thereby impacting the economic stability of the region. The Black Sea is a crucial transit point for global trade, especially for energy exports and agricultural products such as wheat, which are vital for the economies of Ukraine and Russia. The presence of mines disrupts these commercial routes, causing significant economic repercussions.

❖ **Psychological Impact and Uncertainty**: Mines create a psychological effect on both military personnel and civilians. The unpredictability of mine locations makes navigation risky and heightens the sense of insecurity in the region. This uncertainty affects both military operations and commercial activities, amplifying the strategic value of mine warfare beyond its physical impact.

Mine Types and Deployment Methods

The types of mines used in the Black Sea vary from traditional contact mines to more sophisticated magnetic, acoustic, and pressure-activated mines. Traditional mines are relatively simple *(figure 1)* and cheap to produce, while modern mines are equipped with sensors and can be remotely controlled or activated, adding a layer of complexity to mine-clearing operations:

❖ **Contact Mines**: These mines are activated upon direct contact with a vessel. They are typically moored to the seabed and float below the water surface. Both Russia and Ukraine have used contact mines to block access to strategic coastal areas, often in shallow coastal waters or near port entrances to deny access to enemy vessels.

Description: Contact mines are designed to detonate upon direct physical contact with a vessel. They can be moored or free-floating, and are typically placed in areas where enemy ships are likely to pass, such as near ports, harbours, and coastal waters.

Characteristics: Ukrainian contact mines are relatively straightforward in design and are often equipped with chemical or mechanical detonators that trigger the explosive payload upon impact. These mines are less sophisticated than influence mines but are effective in creating blockades or denying access to strategic areas.

Examples: Ukraine has reportedly used several types of contact mines, including Soviet-era models like the KB-1 and KB-2, which have charges of up to 250 kilograms of TNT. These mines are designed to destroy ships by detonating their explosive charge on contact.

❖ **Anchored mines**: These mines are detonated by the influence of the magnetic, acoustic or hydrostatic field of a ship or submarine. They are programmed to detonate only under certain conditions for certain types of ships and submarines.

Description: Anchored mines float at a predetermined depth below the surface. They are designed to detonate upon contact with a vessel or when triggered by specific influences, such as magnetic or acoustic ships signatures.

Characteristics: Ukrainian moored mines are relatively simple in design and include both older Soviet-era mines and newly manufactured types. They are typically equipped with a buoyant mine case connected by a cable to an anchor on the seabed. The mooring cable determines the mine's depth, which can be adjusted to target specific types of vessels (e.g., surface ships or submarines).

Examples: The MYaM and YAM types, both of Soviet origin, are examples of moored mines used by Ukraine. These mines have a charge weight of 200-300 kilograms of TNT and are fitted with contact horns or magnetic triggers that activate upon detecting a nearby ship's magnetic field.

Drifting Mines: mines float freely in the water and can move with currents, making them unpredictable and challenging to locate and neutralize. Several reports suggest that drifting mines have been used by both sides, either intentionally or unintentionally, posing a significant hazard to shipping lanes and coastal infrastructure.

Description: Drifting mines are free-floating mines that move with the currents. Unlike moored mines, they are not anchored to the seabed, making them more unpredictable in their movement.

Characteristics: Ukrainian drifting mines are designed to float at or just below the surface and are equipped with contact detonators. They pose a significant threat to ships due to their mobility, which makes them difficult to detect and neutralize. Drifting mines are typically smaller than moored mines but still carry a substantial explosive charge.

Examples: Some of the drifting mines used by Ukraine are believed to be modified versions of older Soviet-era mines, such as the RM-1. These mines may have been adapted for deployment in shallower waters or near coastal areas to prevent enemy landings or naval incursions.

❖ **Improvised Mines**: Due to the resource constraints faced by Ukraine, there have been reports of improvised explosive devices being deployed as makeshift mines. These can range from modified naval mines to civilian vessels laden with explosives, deployed in a way that allows them to drift into enemy waters.

Deployment methods vary from traditional minelayers, such as ships and submarines, to aerial delivery by aircraft and helicopters. Additionally, modern conflict sees the integration of unmanned vehicles (both aerial and underwater) to deploy or clear mines, showcasing the technological evolution in this area of warfare.



Figure 1: Ukraine's naval mine floating on the Black Sea
(https://odessa-journal.com/turkey-romania-and-bulgaria-have-started-a-joint-operation-for-demining-the-black-sea)

Reasons for the Drift of Ukrainian Mines into Neighbouring Waters

Several factors have contributed to the drift of Ukrainian mines from their original deployment areas to the territorial waters of Romania, Bulgaria, and Türkiye:

❖ **Unanchored or Damaged Mines**:

Explanation: Some of the mines deployed by Ukraine were not properly anchored or were damaged during deployment, causing them to break free and drift with the currents. Strong currents and storm conditions in the Black Sea can dislodge moored mines, transforming them into drifting mines.

Impact: Unanchored or drifting mines pose a hazard not only to enemy vessels but also to neutral ships and coastal infrastructure in the wider Black Sea region. This unintended drift has led to discoveries of Ukrainian-origin mines in Turkish, Romanian, and Bulgarian waters.

❖ **Environmental Factors**:

Explanation: The Black Sea has a specific system of currents, in its entirety, from Kerci to the Bosphorus, through which it connects with the Azov and the Mediterranean Seas. Seasonal weather conditions, including storms and high winds, can exacerbate these currents, causing mines to drift over significant distances.

Impact*:* Environmental conditions such as the Black Sea's north-to-south currents can carry floating mines away from Ukrainian waters into the waters of neighbouring states. The unpredictability of weather patterns and the dynamic nature of the Black Sea's hydrology make it challenging to contain drifting mines to a specific area.

❖ **Deliberate Use of Drifting Mines**:

Explanation: Ukraine has mainly planted anchored and contact mines to protect its maritime waters and Black Sea ports. It is probable that drifting mines are intentionally deployed to discourage Russian military ships or to disrupt maritime transportation routes in disputed areas for civilian purposes.

Impact: The use of drifting mines as a tactical measure could have unintended consequences, with some mines drifting beyond their intended area of operation due to unforeseen changes in wind and current patterns.

❖ **Lack of Effective Mine Management and Disposal**:

Explanation: The conflict's intensity and the urgency of defending coastal areas may have led to a lack of rigorous mine management and disposal practices. Inadequate marking, monitoring, and maintenance of deployed mines increase the likelihood of mines breaking loose and drifting.

Impact: Mines that are not effectively managed or tracked can easily drift into neutral waters, posing risks to maritime navigation and causing international incidents.

Mines Found in the Black Sea in the Last Two Years

As a result of the naval missions, more than 100 sea mines have been discovered and neutralized in the Black Sea in the last two years. The exact number is difficult to determine due to the secrecy surrounding military operations, but various reports and official statements provide some insight:

- Türkiye: As of mid-2023, Turkish authorities reported the discovery of over 30 drifting mines in their territorial waters and international waters near the Bosphorus Strait. These mines were believed to have originated from the conflict zones in the Black Sea and were neutralized by the Turkish Navy's mine-hunting teams.

- Romania and Bulgaria: The Romanian and Bulgarian navies have also reported finding mines drifting into their waters. Romania, for instance, detected and neutralized at least ten mines off its coast in the 2023-2024 period. Bulgaria reported the discovery of four mines in its territorial waters in the same period. These mines have been attributed to the conflict between Russia and Ukraine, carried by currents from areas closer to the warzone.
- Ukraine: Ukraine has been actively engaged in mine-clearing operations along its coast, particularly near key ports like Odessa. Ukrainian sources have reported neutralizing dozens of mines since 2022, mainly moored and contact mines deployed to protect own waters from Russian incursions.

Entities Involved in Mine-Clearing Operations

Several countries and organizations are actively involved in mine-clearing operations in the Black Sea:

- Türkiye: Türkiye, a NATO member with a significant naval presence in the region, has taken an active role in clearing mines, particularly around the Bosphorus Strait. The Turkish Navy operates several mine-hunting ships and has specialized teams trained in explosive ordnance disposal (EOD).
- Romania and Bulgaria: As NATO members, Romania and Bulgaria have coordinated their mine-clearing efforts in the Black Sea with the broader NATO strategy. Both countries have deployed mine-hunting ships and EOD units to detect and neutralize mines drifting into their waters.
- Ukraine: The Ukrainian Navy, supported by international partners, has been involved in extensive mine-clearing operations, particularly around its ports and coastal areas. The Ukrainian Navy uses mine countermeasure vessels (MCMVs) and remotely operated underwater vehicles (ROVs) to locate and neutralize mines.
- NATO and International Organizations: NATO has expressed concerns over the presence of naval mines in the Black Sea and has conducted joint exercises with its member states to enhance mine-countermeasure capabilities. Additionally, organizations like the International Maritime Organization (IMO) monitor and coordinate responses to ensure safe maritime navigation in the region.

Types of Ships Involved in Mine Discovery and Destruction

Various types of ships and naval assets are used in mine-clearing operations in the Black Sea:

- Mine Countermeasure Vessels (MCMVs): These specialized ships are equipped with sonar systems and underwater vehicles to detect, classify, and neutralize mines. The Turkish, Romanian, Bulgarian, and Ukrainian navies have deployed MCMVs in their respective waters to combat the mine threat *(figure 2).*



Figure 2: Mine destroyed by a Romanian War Ship
(https://www.info-sud-est.ro/fotoreport-how-mines-are-destroyed-in-the-black-sea-demonstration-by-romanian-military-divers-five-mines-planted-during-the-war-in-ukraine-were-destroyed-in-romanian-waters/)

- Minehunters: Minehunters are smaller, agile vessels specifically designed to locate mines using sonar and remotely operated vehicles (ROVs). They can safely neutralize mines using explosive charges or mechanical sweeping equipment. The Turkish Navy, in particular, has several minehunters actively patrolling the Black Sea.
- Patrol Boats: Patrol boats equipped with mine detection and clearance capabilities are also used in coastal areas. The Ukrainian Navy has deployed patrol boats around critical ports to ensure safe passage for commercial and military vessels.

- Remotely Operated Vehicles (ROVs): ROVs are unmanned underwater vehicles used to identify and neutralize mines. They can be launched from a variety of ships, including MCMVs, minehunters, and patrol boats. ROVs are also used by all parties involved in mine clearance actions in the Black Sea.

IMPACT ON REGIONAL SECURITY AND INTERNATIONAL TRADE

The use of sea mines the Black Sea, a quite small and closed sea, has significant implications for regional security and international trade. The Black Sea serves as a vital corridor for energy supplies, agricultural and various other commodities exports. Disruption of this maritime traffic impacts not only the littoral states but also global markets. For instance, the blockading of Ukrainian ports has led to shortages and price hikes in global grain markets, given Ukraine's role as a major exporter of wheat and other agricultural products. From a security perspective, the presence of mines creates a contested maritime environment where the risk of miscalculation is high. Neutral shipping, including humanitarian aid missions, faces threats from these hidden weapons. Additionally, the use of mines could potentially draw in NATO, given the Alliance's commitment to maintaining freedom of navigation in international waters and protecting its members' economic interests.

Implications of Mines Drifting to Neighbouring Waters

The drift of Ukrainian mines into the territorial waters of Romania, Bulgaria, and Türkiye has several implications:

❖ **Regional Security Risks**:

Explanation: Drifting mines pose a direct threat to regional security and maritime safety. They can damage or destroy vessels, including civilian ships, fishing boats, and commercial cargo ships. This threat necessitates increased vigilance and mine-clearing efforts by the affected countries.

Impact: The presence of drifting mines has prompted Romania, Bulgaria, and Türkiye to enhance their mine-clearing capabilities, deploying minehunters, patrol boats, and underwater drones to detect and neutralize these threats. These countries have also strengthened their naval cooperation to address the risks posed by drifting mines.

❖ **Diplomatic Tensions**:

Explanation: The unintended drift of Ukrainian mines into neighbouring waters can lead to diplomatic tensions between Ukraine and affected countries.

These incidents may be perceived as violations of territorial sovereignty or as acts of negligence that endanger civilian shipping.

Impact: Diplomatic efforts have been necessary to address these concerns, with Ukraine assuring its neighbours of its commitment to preventing further drift and cooperating in mine-clearing operations. However, the ongoing conflict complicates these efforts, as mines continue to pose a hazard in contested waters.

❖ **Impact on International Shipping and Trade**:

Explanation: The drift of mines into international and territorial waters poses a significant risk to global shipping routes, particularly in the Black Sea, a critical artery for international trade. The presence of mines can lead to the rerouting of ships, increased shipping insurance costs, and disruptions in maritime commerce.

Impact: These disruptions have economic consequences for countries dependent on maritime trade, including Ukraine, Russia, and their neighbours. The international community has called for measures to ensure the safety of shipping lanes and reduce the threat posed by drifting mines.

CHALLENGES IN MINE CLEARANCE

Mine clearance in the Black Sea presents several challenges:

❖ **Technological Complexity**: Modern mines, especially influence mines, require sophisticated technology for detection and neutralization. This technology may not always be readily available or may be limited in capacity, especially for Ukraine.

❖ **Environmental Conditions**: The Black Sea's depth, varying seabed conditions, and water currents complicate mine detection and clearance operations. Mines can drift over time, making their original deployment location irrelevant.

❖ **Political and Military Risks**: Mine clearance operations can be politically sensitive and carry military risks. Clearance operations may be viewed as hostile acts, and there is always a risk of accidental detonation, which could escalate military tensions further.

The International Response

The international community, particularly NATO and other Black Sea littoral states such as Türkiye, Romania, and Bulgaria, has been closely monitoring the situation. These countries have been working to enhance their mine countermeasure capabilities and have engaged in diplomatic efforts to ensure freedom of navigation in the Black Sea. The United Nations and other international bodies have called for adherence to the rules of international law, particularly the United Nations

Convention on the Law of the Sea (UNCLOS), which governs the use of mines in international waters.

However, geopolitical divisions have complicated a unified response. While NATO and the European Union have supported Ukraine, Russia continues to assert its right to deploy mines within its claimed territorial waters. The lack of a clear international mandate for mine clearance in disputed waters adds to the complexity of addressing the issue.

FUTURE OF MINES WARFARE IN THE BLACK SEA

The future of mine warfare in the Black Sea is likely to be shaped by several factors *(figure 3)*:

❖ **Technological Advancements**: The development of more sophisticated mines and mine-clearing technologies will play a crucial role. Advanced mines with stealth capabilities and multi-sensor triggering mechanisms could be used to enhance naval blockades or deny access to key areas. Conversely, improvements in mine detection and neutralization technologies, such as autonomous underwater vehicles (AUVs) and AI-driven sonar systems, will enhance the ability to counter these threats.

❖ **Regional Cooperation and NATO Involvement**: Continued cooperation among Black Sea states, along with NATO's presence in the region, will be critical in mitigating the mine threat. Joint exercises and shared intelligence can enhance collective security and response times to drifting or newly deployed mines.

❖ **Legal and Diplomatic Measures**: Efforts to establish international norms and legal frameworks to prohibit the indiscriminate use of mines, particularly drifting mines, could reduce the threat over time. Diplomatic efforts to end hostilities in the Black Sea region would also decrease the likelihood of continued mine warfare.

❖ **Environmental and Economic Implications**: The extensive use of mines in the Black Sea poses environmental risks, including damage to marine life and habitats. Furthermore, the presence of mines can disrupt shipping routes, leading to economic losses for countries dependent on maritime trade. Future strategies must consider these implications to ensure sustainable and safe navigation in the region.

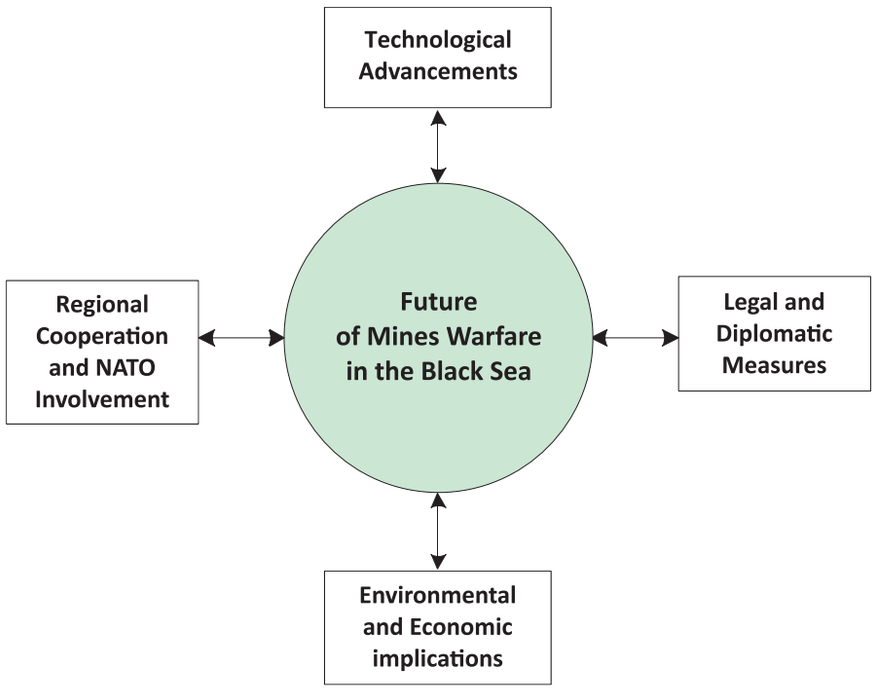


Figure 3: Factors of the future of mines warfare in the Black Sea (author's design)

CONCLUSIONS

The *"Mines War"* in the Black Sea is a microcosm of the broader conflict between Russia and Ukraine, highlighting the evolving nature of naval warfare and the strategic use of mines in modern conflicts. The deployment of mines serves multiple purposes, from denying access and disrupting economic activities to creating psychological uncertainty. The conflict underscores the need for enhanced mine countermeasure capabilities, better international cooperation, and adherence to international maritime law to prevent further escalation and ensure safe navigation in this strategically vital region.

The *"Mines War"* in the Black Sea is a major component of the conflict between Russia and Ukraine. The use of various types of mines, together with the complexity of mine operations, presents important threats to regional security and safety of shipping. The future of war with mines in the Black Sea will depend on technological advancements, regional cooperation, and diplomatic efforts to address the root causes of the conflict. The use of naval mines by Ukraine in the conflict with Russia

has had unintended consequences, with some mines drifting into the waters of neighbouring countries such as Romania, Bulgaria, and Türkiye. Various factors, including environmental conditions, inadequate mine management, and the deliberate use of drifting mines, have contributed to this phenomenon. The drift of mines poses significant security, diplomatic, and economic risks, prompting affected countries to enhance their mine-clearing capabilities and engage in diplomatic dialogue with Ukraine. As the conflict continues, the threat of drifting mines remains a great challenge to the security of the Black Sea basin.

BIBLIOGRAPHICAL REFERENCES:

1. Bulgarian Naval Forces (2023). *Mine Clearance and Maritime Safety Efforts in the Black Sea*.
2. Delanoë, I. (2024). *Russia's Black Sea Fleet in the "Special Military Operation" in Ukraine*, https://www.fpri.org/article/2024/02/russias-black-sea-fleet-in-the-special-military-operation-in-ukraine/, retrieved on 17 August 2024.
3. Greenpeace (2024). *Black Sea: Shadow of the Mines OMV to Build Gas Platforms and Pipelines Amidst Black Sea War Zone*, https://www.greenpeace.org/static/planet4-romania-stateless/2024/06/7b5c64be-en_mines_risk_analysis_black_sea.pdf., retrieved on 12 May 2024.
4. International Maritime Organization (IMO), (2023), *Safety of Navigation in the Black Sea: Current Threats*.
5. Jane's Defence Weekly (2023). *Naval Mines in the Russia-Ukraine Conflict: Types, Deployment, and Drift Pattern*.
6. NATO Maritime Command Reports on Mine Warfare in the Black Sea.
7. *The Drifting Menace*, https://www.rand.org/pubs/commentary/2022/11/the-drifting-menace.html, retrieved on 13 July 2024.
8. Turkish Ministry of Defense, (2023), *Naval Mine Clearance Operations in the Bosphorus Strait*.
9. Ukrainian Navy Official Reports (2022-2023). *Mine Deployment and Management Strategies in the Black Sea*.
10. Yaylali, C.D. (2024), *Three NATO allies activate Black Sea task force,* https://www.defensenews.com/author/cem-devrim-yaylali/, retrieved on 29 June 2024.
11. https://odessa-journal.com/turkey-romania-and-bulgaria-have-started-a-joint-operation-for-demining-the-black-sea, retrieved on 29 June 2024.
12. https://www.fpri.org/article/2024/02/russias-black-sea-fleet-in-the-special-military-operation-in-ukraine/, retrieved on 12 May 2024.

13. https://www.info-sud-est.ro/fotoreport-how-mines-are-destroyed-in-the-black-sea-demonstration-by-romanian-military-divers-five-mines-planted-during-the-war-in-ukraine-were-destroyed-in-romanian-waters/, retrieved on 13 July 2024.

RECRUITMENT AND SELECTION OF HUMAN RESOURCES IN TODAY'S DYNAMIC ENVIRONMENT – DEFINITIONS, FEATURES AND TRENDS –

Assistant Professor Nehridzhan Arif MEHMED, PhD

"Georgi Benkovski" Air Force Academy,
Dolna Mitropolija, Bulgaria
DOI: 10.55535/RMT.2024.4.21

The article shares some essential aspects related to the recruitment and selection of human resources in today's dynamic environment. Definitions of their essence are given and the main steps in recruitment and selection of human resources are highlighted. An attempt was made to examine the activities related to recruitment and selection of personnel in both business and military organizations. Some trends and perspectives in this direction are indicated. Emphasis is placed on the strategic role of recruitment and selection of suitable personnel in business organizations. Given the dynamics in the modern environment, some weaknesses in the recruitment and selection of human resources in business organizations are indicated and ideas for their improvement are proposed.

Keywords: human resources; recruitment; management; selection; business organizations;

INTRODUCTION

The changes that have occurred in recent years in the modern environment provoke an increase in the role of activities related to human resources management and, more specifically, recruitment and selection of human resources. They become a strategic tool with a number of opportunities provided to all sectors, especially the military and business units, to achieve good business results.

The dynamics in the modern socio-economic conditions reinforces the discrepancy between the possessed knowledge, skills and attitudes of human resources and the growing requirements for the performance of labour activities. It brings to the fore the strategic role of recruitment and selection activities, especially for business and military organizations, which are considered in the present study.

The management of human resources and the activities of recruitment and selection of human resources in business organizations as well as in military ones attract the interest of a number of Bulgarian and foreign authors and researchers. In business practice, increasing attention is paid to the effective provision of suitable personnel. It requires clarifying the nature of human resource recruitment and selection activities. In the increasingly complex and dynamic environment, business organizations have an ever-increasing need for recruitment and selection of human resources able to achieve effective results.

With regard to highlighting the weaknesses in the implementation of the activities related to the recruitment and selection of suitable personnel, the business organizations from the sectors *"Transportation and storage"* and *"Hotels and restaurants"* are examined.

The main goal is to reveal the essential aspects of recruitment and selection of human resources, to highlight some features, trends and perspectives in this direction, to reveal some advantages and weaknesses of activities related to recruitment and selection of human resources in the sector *"Transportation and storage"* and in sector *"Hotels and restaurants"*, and to present ideas for their improvement.

There are several reasons to choose the sector *"Transportation and storage"* and in sector *"Hotels and restaurants".* On the one hand, organizations in the sectors face challenges related to the dynamics of the modern business environment, as a result of which they find it difficult to secure suitable personnel for the sector.

On the other hand, the shortage of well-prepared personnel in sector *"Transportation and storage"* and in sector *"Hotels and restaurants"* requires attention to be paid to the activities related to the recruitment and selection of human resources.

RECRUITMENT AND SELECTION OF HUMAN RESOURCES – ESSENTIAL ASPECTS

In today's conditions, the drive to provide suitable personnel in business organizations from various sectors of the economy is distinctive. With the dynamics in the business environment, the importance and role of activities related to the recruitment and selection of human resources for business organizations are growing. It gives rise to the interest of a number of authors and researchers in revealing the essential aspects of the recruitment and selection of human resources in a number of definitions presented in various scientific developments.

In this regard, Michael Armstrong believes that recruitment is the process of finding and hiring the people the organization needs. Selection is that part of the recruitment process concerned with deciding the applicants or candidates that should be appointed to jobs. Recruitment can be costly (Armstrong, 2014). The author's definition is presented relatively fully. It assumes that human resource selection is a part of the human resource recruitment process.

Yosif Iliev and Kaloyan Dimitrov define the activity of recruiting human resources as a natural step in the effective management of human resources. According to the authors, the recruitment activity is followed by a long process of selection of human resources in the business organization (Iliev, 2014).

Another perspective argues that human resource management (HRM) can be considered in both civilian and military organizations as a set of activities and responsibilities related to personnel and aimed at the optimal deployment of employees to contribute to the performance of the organization. In this regard, HRM includes activities such as recruiting, selecting, hiring, training, remuneration, fringe benefits, assessment and development, and outflow or dismissal of employees, as well as the welfare and health of subordinates (Boselie, 2014; Dessler, 2021; cited in: Tessa op den Buijs, 2023, p. 2). The activities related to recruitment and selection of human resources stand out as the first.

Shopov, Evgeniev, Kamenov, Atanasova and Bliznakov point out that the management of human resource is a continuous and purposeful process that starts with the attraction and selection of the most suitable people for the respective positions and jobs (Shopov, 2015). An idea is formed that recruitment and selection of human resources are activities in which a certain sequence of actions is observed

to achieve the set goals, according to the established standards of work in the business organization.

The views of the authors Shopov, Evgeniev, Kamenov, Atanasova and Bliznakov on the issue of human resources selection are interesting. The authors believe that selection and placement can generally be defined as the process of attracting the right candidates for a certain position, assessing their qualities from the point of view of the position, the unit and the business organization as a whole, deciding who to make job offer and appointing the selected persons (Ib.). The definition thus presented is wide-ranging as it also refers to the appointment of the selected candidates to the respective posts and jobs.

According to David A. De Cenzo, Susan L. Verhulst, Stephen P. Robbins, the human dimension of organizational management, including acquiring employees, developing their skills, motivating them to higher levels of performance, and ensuring that they continue to maintain their commitment to the organization is essential to the achievement of organizational goals. It applies regardless of the type of organization – government, business, education, healthcare, recreation or other social activity (De Cenzo, 2016). In this sense, the acquisition of human resources is aimed at achieving the goals of the business organization.

According to Gary Dessler, recruitment and selection start with workforce planning and forecasting. Workforce planning is the process of deciding what positions the firm will have to fill, and how to fill them. It often starts by forecasting personnel needs, perhaps using trend analysis, ratio analysis, scatter plots, or computerized software packages. A significant moment is forecasting the supply of inside candidates. Forecasting the supply of outside candidates is important too, particularly when unemployment is low and good candidates are more difficult to come by (Dessler, 2017, p. 157).

It is necessary to make the distinction that the recruitment of human resources is an activity that provides an opportunity to acquire the number and quality of people necessary to ensure the continuity of the workflow in the organization and the achievement of the organizational goals (Iliev, 2021). In contrast to the recruitment of human resources, the selection of human resources is defined as the activity of choosing a suitable candidate who corresponds to the greatest extent to the requirements of the job (Ib.).

Considering the mentioned definitions of recruitment and selection of human resources and taking into account the significant moments in them, according to us, recruitment of human resources is generally a process of attracting the most suitable people to the relevant positions and jobs in a business organization,

while selection is a continuous and purposeful process of selecting and appointing human resources, according to their qualities, knowledge and skills, in accordance with current and future needs of the workplace, in the structural unit and in the business organization.

In the modern business environment, the effective recruitment and selection of human resources cannot be achieved only on the basis of a good knowledge of their nature. It is necessary to highlight the main steps (elements) in their implementation.

In this regard, despite the fact that there is a difference in the definition of the two concepts (recruitment of human resources and selection of human resources), several steps in their application stand out. As far as they are concerned, these steps are presented in *table 1.*

Table 1: The stages of recruitment and selection (Armstrong, 2014)

No	**The stages of recruitment and selection**
.1	Defining requirements
.2	Attracting candidates
.3	Sifting applications
.4	Interviewing
.5	Testing
.6	Assessing candidates
.7	Obtaining references
.8	Checking applications
.9	Offering employment
.10	Following up

Undoubtedly the first activity is defining requirements. Requirements are set out in the form of role profiles and person specifications. These provide the information required to post vacancies on the company's website or the internet, draft advertisements, brief agencies or recruitment consultants and assess candidates by means of interviews and selection tests (Armstrong, 2014).

The second step is attracting candidates. In this case the following steps are required when planning how to attract candidates: analyse recruitment strengths and weaknesses to develop an employee value proposition and employer brand; analyse the requirement to establish what sort of person is needed; identify potential sources of candidates (Ib.).

The next step is dealing with applications – if recruitment agencies or consultants are used, they will deliver their client a shortlist of candidates for interview. If not, the organization has to sift the applications itself. This means examining the information supplied by applicants, sorting them and drawing up a shortlist of applicants to be interviewed (Ib.).

A very significant step are the selection methods – the aim of selection is to assess the suitability of candidates by predicting the extent to which they will be able to carry out a role successfully – interviewing, testing (Ib.).

The following activity deserves attention – provisional offers and obtaining references. The main purpose of a reference is to obtain in confidence factual information about a prospective employee (Ib.).

As the next steps stand out – checking applications, offering employment (the final stage in the selection procedure is to confirm the offer of employment after satisfactory references have been obtained, and the applicant has passed the medical examination required for pension and life assurance purposes or because a certain standard of physical fitness is required for the work. The contract of employment should also be prepared at this stage), following up (it is essential to follow up newly engaged employees to ensure that they have settled in and to check on how well they are doing; following up is also important as a means of checking on the selection procedure) and dealing with recruitment problems (Ib.).

Gary Dessler believes that the job analysis identifies the duties and human requirements of each of the company's jobs. The next step is to decide which of these jobs one needs to fill, and to recruit select employees for them. According to the author, the recruiting and selecting process can be envisioned as a series of hurdles (*figure 1*), (Dessler, 2017, p. 128).

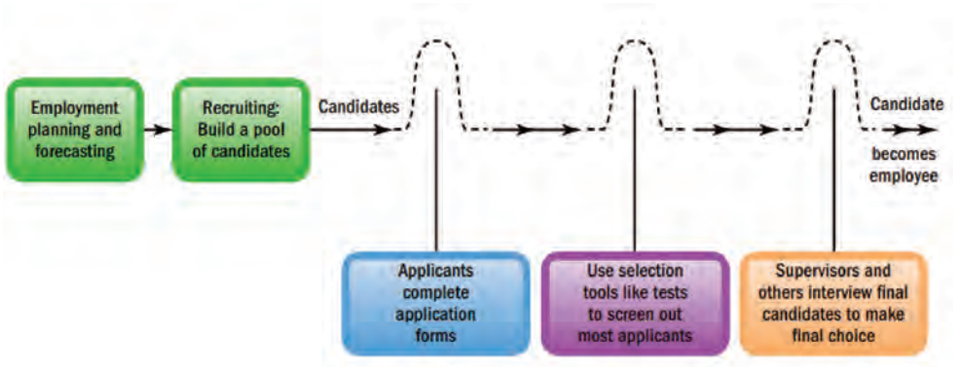


Figure 1: Steps in Recruitment and Selection Process (Ib.)

It is noteworthy that, as a first step in deciding what positions to take, emphasis is placed on planning and forecasting. An essential point of the author's proposal is building a pool of candidates for these jobs, by recruiting internally or externally candidates and having candidates' complete application forms and perhaps undergo initial screening interviews. The final steps in recruitment and selection of human resources include the use of selection tools like tests, background investigations, and physical exams to screen candidates and decide to whom to make an offer, by having the supervisor and perhaps others interview the candidates (Ib.).

Based on the literature review, it can be summarized that:

- In the economic literature, there are definitions of a number of authors for the activities of recruitment and selection of human resources. They emphasize certain aspects of these concepts (recruitment and selection of human resources) that are significant for the activity of the business organization.
- The opinions of authors regarding the steps (elements) of recruitment and selection of human resources are presented. The activities in these elements are interconnected and it is imperative that they continuously adapt to changes in the modern environment.

RECRUITMENT AND SELECTION OF HUMAN RESOURCES IN TODAY'S DYNAMIC ENVIRONMENT – TRENDS

Regarding the national practice, some elements related to the recruitment and selection of human resources are presented. In this regard, the number of employees under labour contract in business organizations, which, according to the Classifier of economic activities 2008 (KID 2008), are included in sector *"Transportation and storage"* and in sector *"Hotels and restaurants"* is presented. For the purposes of this report the period from 2018-2023 is covered.

For the researched period (2018-2023), business organizations in the country with economic activity in the sector *"Transportation and storage"* report a change in the number of employees labour contract. It is noteworthy that their number decreased significantly in the second half of the period 2018-2023 (*figure 2*).

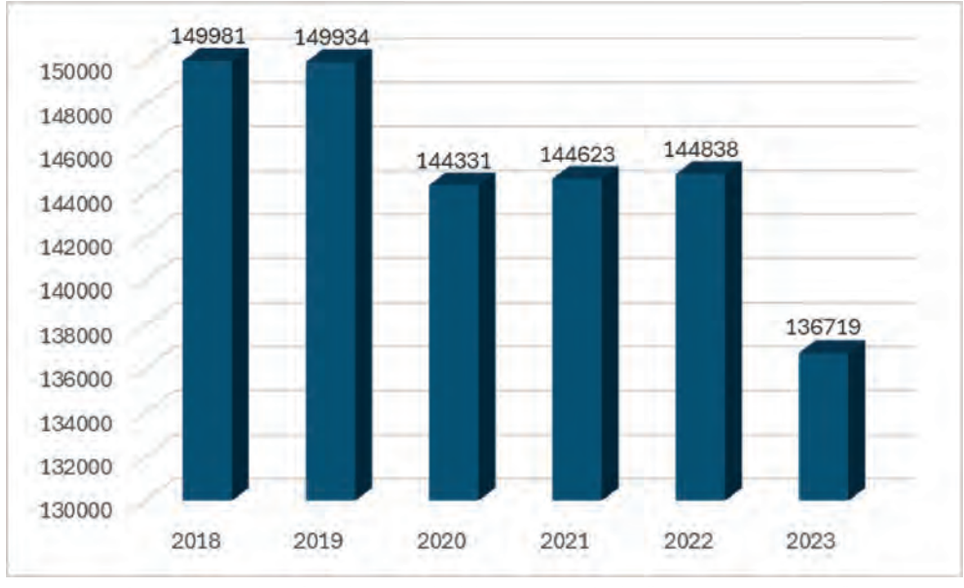


Figure 2: Average number of employees under labour contract in the "Transport and storage" sector for the period 2018-2023
(Adapted from the National Institute of Statistics (BG), 2024, Preliminary data for 2023)

Figure 2 shows that for 2023, compared to 2018, there is a decrease in the number of employees under labour contract in the considered sector – with a negative growth rate (0.09%). For the period under review, the largest decrease in the number of employees under a permanent employment contract in the sector was in 2020 – a negative change of 0.04% was observed compared to 2018 (National Institute of Statistics, 2023 – own calculations based on NIS data).

For the research period (2018-2023), a similar dynamic in the number of employees under labour contract is also observed in the sector *"Hotels and restaurants" (figure 3).*

Figure 3 shows that the number of people employed under labour contract in the sector is decreasing. For 2023, compared to 2018, the change is 0.22%. It is noteworthy that at the end of the same period (in 2023) there is a positive trend in the number of employees compared to 2020 – a positive growth rate (0.04%) stands out (National Institute of Statistics, 2023 – own calculations based on NIS data). The change in the number of employees in the sector is weak.

It means that the impact of the Covid-19 pandemic that occurred in 2019 is significant, due to which problems arise related to the preservation and procurement of human resources in business organizations from both sectors. The consequences reflect on the human resource management system in the business organizations

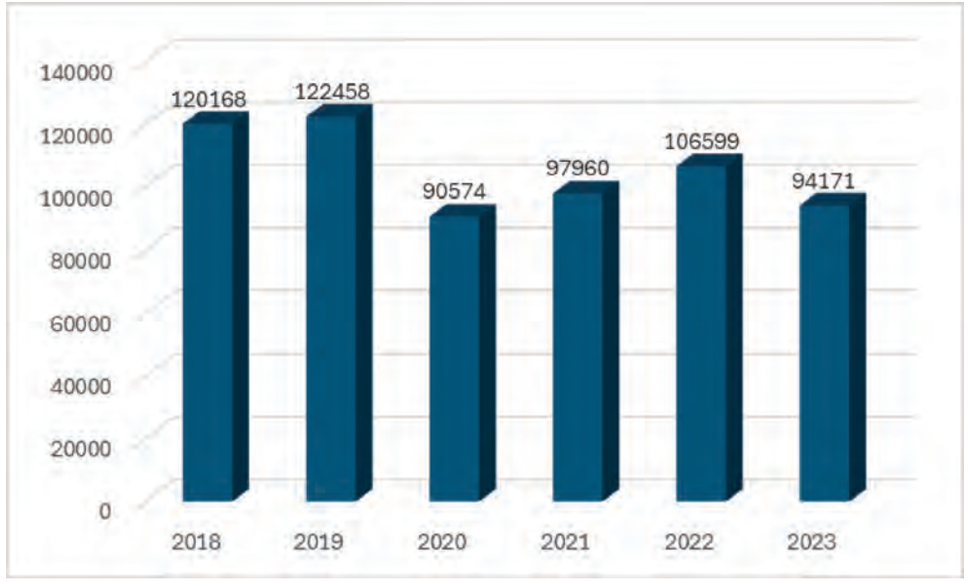


Figure 3: Average number of employees under labour contract in the "Hotels and restaurants" sector for the period 2018-2023
(Adapted from the National Institute of Statistics (BG), 2024, Preliminary data for 2023)

of the sectors and more specifically on their policy for the necessary personnel at work.

For the selected period in Bulgaria, the total costs of employers for labour in the *"Transportation and storage"* sector and in the *"Hotels and restaurants"* sector are characterized by significant changes. For example, in the third quarter of 2023 compared to the third quarter of 2022, the total costs of employers for one hour worked by their employees increased by 15.1% (according to preliminary data). Among the economic sectors with the highest recorded growth in total labour costs are *"Hotel and restaurant industry"* – by 18.8%, and *"Transport, warehousing and post"* – by 17.4% (National Institute of Statistics, 2024).

On the one hand, the variable demand for the services provided in the specified sectors, caused by the pandemic and its consequences, directs the efforts of the managers of business organizations to follow strategies to improve the quality of the activities performed. Such efforts are accompanied by meeting the needs of professionally trained personnel. On the other hand, the recovery of the considered sectors of the economy after the pandemic leads to a new environment of cooperation, investment, information, innovation, adaptability.

As for HRM practices in the military, they are fundamental to promoting an effective and efficient organization. The military invests heavily in recruiting

and selecting potential candidates, training and development, management of performance, the compensation process and benefits, as well as working atmosphere and employee relations. These practices help ensure that personnel are ready for their jobs, can perform at a high level, and remain motivated and engaged (op den Buijs, 2023, p. 16).

In recent years, important trends relevant for the field of HRM are further IT developments and digitalization, environmental or climate changes, and labour market trends to which organizations have to adapt. For example, there is an increasing attention to sustainable HRM (Müller, 2018; op den Buijs, 2023) and green HRM (O'Donohue, 2016; op den Buijs, 2023). These trends also lead to new directions in HRM (op den Buijs, 2023, pp. 4-5).

They direct employee development so they can perform their jobs with dedication and efficacy, be motivated, and experience job satisfaction. Ideally, both employer and employee are satisfied and know what they gain from each other (Boselie 2014; op den Buijs, 2023).

In most organizations, HRM departments and HR specialists support the line managers. These specialists assist in recruiting, hiring, training, evaluating, and promoting and rewarding personnel, as well as employee safety and health at all levels, among other things. Today, there are many trends that require HR specialists to take a more strategically important role in organizations. All kinds of influences from the environment are causing HRM to change. These influences include technological change, increasing workforce diversity, a new generation of young people and their motivation, the labour market, globalization, and economic influences (op den Buijs, 2023).

In this regard, the need for recruitment and selection of suitable human resources is increasing. It gives rise to the need to study the activities of recruitment and selection of human resources. For their effective implementation, it is necessary for the heads of business organizations to pay attention to the elements of the activities of recruitment and selection of human resources, to highlight the advantages and disadvantages and to look for ways to improve them.

It can be summarized that:

Firstly, on the state of human resources in the *"Transportation and storage"* sector and in the *"Hotels and restaurants"* sector:

- The number of persons employed under a permanent employment contract in the *"Transport, warehousing and post"* sector for the period 2018-2023 has decreased. There is a tendency, although weakly expressed, towards an increase in the number of people employed in the sector. The reasons for the reduction are a reflection of the pandemic and its consequences.

- A similar dynamic in the number of persons employed under a permanent employment contract in the *"Hotels and restaurants"* sector is observed for the considered period 2018-2023. At the end of the considered period, an increase in their number is observed.

Secondly, total labour costs for both sectors have increased.

Thirdly, the factors of the modern dynamic environment that have an impact on the activities related to the recruitment and selection of human resources, in business organizations, are very diverse, but through their observance and successful reporting, the set goals can be met. It is also necessary to respond in a timely manner to the challenges that have arisen in relation to the recruitment and selection of suitable personnel, namely application of various methods and means for recruitment and selection of suitable human resources.

GUIDELINES FOR IMPROVING HUMAN RESOURCES RECRUITMENT AND SELECTION ACTIVITIES

After the conclusions and summaries for the recruitment and selection of human resources in the business organizations in the *"Transportation and storage"* sector and in the *"Hotels and restaurants"* sector, some advantages and weaknesses of these processes are highlighted. Eliminating weaknesses and increasing strengths allows increasing the efficiency of recruitment and selection of human resources. Opportunities to improve recruitment and selection of human resources should be considered in the following sequence:

- Revealing the prerequisites for improving the activities related to the recruitment and selection of human resources in the *"Transportation and storage"* sector and in the *"Hotels and restaurants"* sector. They are related to the requirements of the European organizations, as well as the national organization, the peculiarities and requirements of the labour market at the local level, the legal framework of the country, the dynamics of the technical and technological state, the availability of investments, the growth of commodity markets etc.
- With the continuous development of technical progress and changing market conditions, it is expected that the right candidates can be attracted and selected. In this regard, a wider application of flexible methods of recruitment and selection of human resources and implementation of more effective and continuous feedback on the achieved results are necessary.

CONCLUSIONS

In the modern economic reality, the role of recruitment and selection of human resources in business organizations as well as in military ones, both locally and internationally, is significant. This is due to the built strategies that organizations follow. Similar characteristics stand out for business units operating in the *"Transportation and storage"* sector and in the *"Hotels and restaurants"* sector.

In this regard, some essential aspects of recruitment and selection of human resources have been studied and defined in a theoretical aspect, a definition has been derived and the main steps in recruitment and selection of human resources have been highlighted. A study of the trends in the average number of employed persons, labour costs in business organizations from the two analysed sectors. Opinions are shared on some perspectives regarding the activities related to the recruitment and selection of suitable personnel, and some features of the same activities. For this purpose, statistics, reports, publications related to human resources management have been used. The results of the conducted theoretical studies give reason to summarize that the effectively implemented activities of recruitment and selection of human resources provide suitable personnel, helping to overcome risky situations and achieve significant success in modern business conditions.

BIBLIOGRAPHY:

1. Armstrong M., Taylor S. (2014). *Armstrong's Handbook of Human Resource Management Practice*. 13th edition. London.
2. Boselie, P. (2014). *Strategic human resource management. A balanced approach*. London: McGraw-Hill Education.
3. DeCenzo, D.A., Robbins, S.P., Verhulst, S. (2016). *Fundamentals of human resource management*. 12th edition. USA.
4. Dessler, G. (2017). *Human Resource Management Practice,* 15th Edition.
5. Iliev J. (2014). *Управление на човешките ресурси*. София: ИК – УНСС; (2014). *Human resource management*. Sofia: IC – UNSS.
6. Iliev, Y., Dimitrov, K. (2021). Управление на човешките ресурси. София; (2012). *Human resource management*. Sofia.
7. Müller, M., Kiel, D., & Voigt, K. I. (2018). *What drives the implementation of industry 4.0? The role of opportunities and challenges in the context of sustainability. Sustainability*, pp. 10, 247.
8. National Institute of Statistics of Bulgaria (BG), 2024.
9. op den Buijs, T., Olsthoorn, P. (2023). *Human Resource Management for Military Organizations: Challenges and Trends*, Netherlands.
10. O'Donohue, W., & Torugsa, N. A. (2016). *The moderating effect of 'green' HRM on the association between proactive environmental management and financial performance in small firms*. International Journal of Human Resource Management, pp. 27, 239–261.
11. Shopov D., Atanasova, M. (2015). *Управление на човешките ресурси*. София: Тракия-М; (2015). *Human resource management*. Sofia: Trakia-M.

HUMAN RESOURCES AND THEIR MOTIVATION WHEN CHOOSING A MILITARY PROFESSION

Associate Professor Galina TODOROVA, PhD
Department of Natural Sciences and Humanities,
Air Force Academy, Dolna Mitropolia, Bulgaria
DOI: 10.55535/RMT.2024.4.22

Human resources are a key component for any organization, including military structures, because their functioning guarantees the national security of countries!

At the present time, in the conditions of uncertainty and active wars, the choice of a military profession by young people is a difficult process and depends on their personal growth, social environment and beliefs.

The purpose of this article is to examine motivation as a process and the motivating factors of young people in Bulgaria when choosing a military profession.

The main hypothesis defended through this article is that properly motivated people will defend their country worthily and work for the peaceful resolution of regional and international conflicts.

The main instrument for data collection is a survey conducted on 50 cadets who have chosen to study in various military specializations.

The main conclusions we reach is that the motivation of human resources in choosing a military profession is complex and includes personal, economic, psychological and social factors, and armed forces that invest in motivated human resources for the future will be more effective and successful in war and in maintaining peace in a regional and global context!

Keywords: human resources; military profession; motivation; NATO; Bulgaria;

INTRODUCTION

The global security environment has a significant impact on Bulgaria in many aspects – from migration crises to cyber threats and regional instability. In this context, Bulgaria should continue to strengthen its internal security structures, actively participate in international organizations such as NATO and the EU, and work to prevent new threats through cooperation and adaptation to the changing global situation. It has to do with the management of various resources, which are a set of human, material, technological and financial elements that guarantee the country's ability to protect its security and fulfil its international commitments. It is known that Bulgaria maintains a defence policy in accordance with the basic laws of the country – the Constitution, the Plan for the Development of the Armed Forces of the Republic of Bulgaria until 2026, the Programme for the Development of Defence Capabilities until 2032, constantly increasing its defence spending, which is 2% of the country's gross domestic product: *"NATO includes only 16% of all countries with 32 member states. Last year, the member countries were responsible for 55% of all global military spending, with the USA accounting for more than two-thirds of that total. At the 2023 Vilnius Summit, NATO leaders approved a new Defence Investment Pledge, making an enduring commitment to investing at least 2% of GDP annually on defence. The new Defence Investment Pledge also calls for Allies to meet 20% of annual defence expenditure guideline on major new equipment, including research and development."* (Funding NATO, 2024).

Graphically, these costs are shown by year and country in *figure 1.*

The Armed Forces of the Republic of Bulgaria consist of three main types of troops that ensure the defence of the country – by land, air and sea. But one of the main problems of the Bulgarian armed forces is the shortage of personnel. Bulgaria faces challenges with attracting and retaining sufficient qualified personnel in the military, which is related to socio-economic factors and competition from other professional sectors.

From a theoretical point of view, there is a difference between the concepts of personnel and human factors. It is customary for the term *"personnel"* to refer to people as an organizational unit that perform specific tasks and roles, and the term *"human factor"* to emphasize the behaviour and interactions of people with the environment, systems and technology, with the aim of understanding

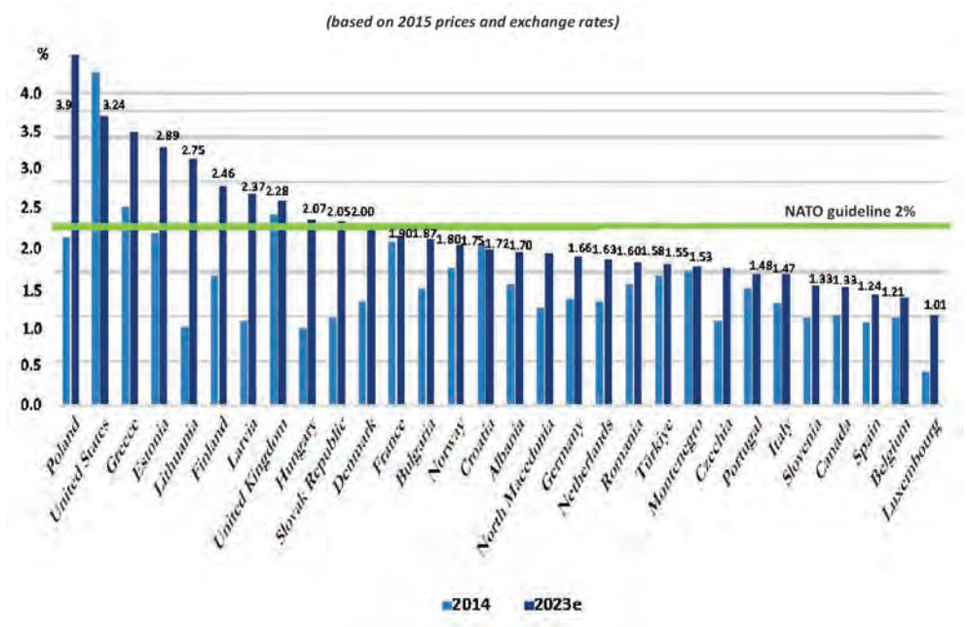


Figure 1: Defence expenditure as a share of GDP (%) (Ib.)

how their actions can affect performance and safety in different directions. In the socio-economic literature, the main authors who have worked on the researched issues are: Gary Dessler, David Ulrich, John Storey, Donald Norman, James Reason, Paul Fitts, Hal Hendrick. In Bulgaria, the researchers in this field are: Veselin Dimitrov, Georgi Popov, Ivan Panchev, Rumen Manolov, Valentin Zhekov and others. In order to support the processes of recruiting quality people and specialists in the armed forces, the main goal of this study is to analyse the human factor and their motivation when choosing a military profession.

THE ESSENCE OF MOTIVATION AS A PROCESS

Motivation is a complex psychological process that explains how and why people engage in certain activities and how their efforts and behaviours are aimed at achieving certain goals. In the armed forces, the problem of people's motivation occupies an increasingly significant place in the field of human resources management, since the subject of management is precisely people – the most important and powerful factor for the development of defence activities. The emphasis is placed on military personnel and civilian employees to be motivated and stimulated to work, which, in turn, will lead to the preservation of peace and guarantee better economic results for the country. Therefore, it is necessary to pay

more and more attention to improving quality and motivation. The basic foundations of professionalism in the field of dangerous professions are (Bakhtyorovich, 2020):

- Assuming responsibility for a personal decision;
- The highest organization;
- Personal courage;
- Self-criticism;
- Sociologization of motives for actions.

In the course of the presented aspects on the essence of the concept of motivation, the main types of motivation are consistently determined, as a result of which it is unified that internal motivation in unison with external motivation contributes to the favourable impact on the individual and organizational level, which in most cases leads to motivational progress in the labour process.

Table 1: Conceptual views related to motivation (adapted from Stefanova, 2020, p. 130)

Period	Author	Views related to motivation
17th century	Benedict Spinoza; Thomas Hobbes; Renee Descartes	Descartes speaks of *"free will"* and of *"spontaneity of the volitional impulse"*. Spinoza sees *"the pulls"* as the main instigator of action. Hobbes chooses the instinct for self-preservation and profit.
The 20s and 30s of the 20th century	William McDougall	Motivation is innate and coincides with the innate instincts of the person.
30s and 40s of the 20th century	Kurt Lewin; Henry Murray; Abraham Maslow	Lewin explains behaviour based on the relationship between the individual and the specific situation. According to Murray, the variety of needs can motivate behaviour for a certain time. Maslow points out that a person has a desire to satisfy a predetermined scheme of needs, among which there is a hierarchy.

Period	Author	Views related to motivation
The 50s of the 20th century	Frederick Herzberg; Douglas McGregor	Herzberg determines that motivation is triggered by two factors: the first is the specific environment of work (working conditions, pay), and the second brings job satisfaction. McGregor's theory is based on two opposing models. The first model, which to some extent gives a negative image to the employee, is called theory X. The other positive model is named theory Y.
The 60s of the 20th century	Clayton Alderfer; Elizabeth Duffy; Stacey Adams; Victor Vroom; Lyman Porter and Edward Lawler; Jack Brehm	Alderfer, in the inciting-motivational sphere of the psyche, distinguishes two levels – *"motives for need"* (lower) and *"motives for development"* (higher). Duffy emphasizes ideas about knowledge and activation like elements intermediate motivation and action. According to Adams, it is present a directly proportional connection between equality and motivation. Vroom determines motivation like possible only when there is a clear link between the work performance and the result and when that result is perceived like means to meet some need. Porter and Lawler summarize that there are two factors on which effort on individual input in the labour depend: value on remuneration and expectations about the relationship between effort and reward. Brehm makes supposition that *"given the degree to which the individual is aware of his or her needs and what is necessary to achieve them, he/she will choose behaviour that maximizes the satisfaction of the needs"*.

Period	Author	Views related to motivation
The 70s of the 20th century	Clayton Alderfer, David McClelland, Gary Latham & Edwin Locke	According to Alderfer, motivation is built on the basis of a three-level hierarchy of needs and their overcoming depends on the will and capabilities of the individual. McClelland argues that all motives and needs of human without exception themselves are acquired and formed in the course of his development. According to the theory of Latham and Locke, two characteristics of the objectives are particularly important – difficulty and clarity. Up to a certain limit, the difficulty of the goal can be motivating, but when it is crossed, the goal is perceived as unattainable and the motivational charge sharply drops.

Each of these theories reveals essential characteristics of motivation as a process, but the motivating factors for each person are strictly specific and different.

THE MAIN MOTIVATING FACTORS WHEN CHOOSING A MILITARY PROFESSION

The choice of the military profession is connected to many factors. Charles Handy, in his book *"Understanding Organizations"* (1976), outlined three factors that influence motivational decisions and subsequent behaviour:

- *Needs* – which are the most significant among them?
- *Expectations* – how will we get the desired results through certain actions?
- *Results* – how will the consequences of our actions contribute to meeting our needs?

The factors are different and strictly individual for each person and the most important are:

- Moral and ethical motives of patriotic duty and/or family tradition and heritage, pride in belonging to the nation. Relatives who were military can be a role-model for military career.
- Desire for personal development of leadership skills, physical endurance, discipline, professional skills and self-improvement, as well as an international career in the joint command.

- Social security and stability – providing housing, receiving a regular salary, early retirement and other social benefits.
- From participating in international missions to completing complex tasks, the armed forces offer a dynamic environment.
- Opportunities for vocational training and advancement through language training and participation in other specialised trainings and courses that can help employees develop new skills and advance their careers.
- Group affiliation and teamwork to build strong relationships with colleagues can be motivating.
- Opportunity for social connections and new acquaintances, creation of new social connections and acquaintances with people from different backgrounds and cultures.

In relation to these factors, a survey was conducted among a 50-people target group aged 19 to 24 on *"What was the main reason why you chose the military career?"* The answer of respondents was: Patriotism – 30%, Financial security – 45%, Personal development – 15 %, Family traditions – 5%.

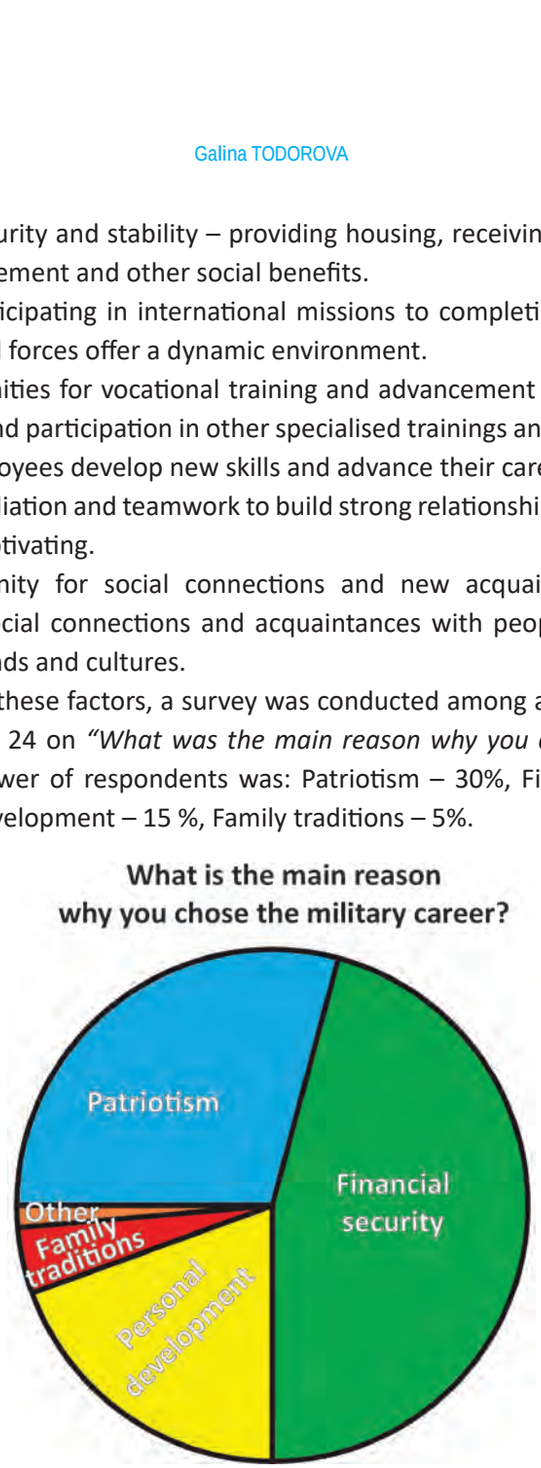


Figure 2 (author's design)

In Bulgaria, according to the National Statistical Institute, the average salary for 2023 is BGN 2,296. This tendency, I believe, is characteristic of professional armed forces. According to Jared Keller, who analysed the same aspect, *"Americans join the Army for plenty of reasons: for country, family, and honour. According to a new study of enlisted soldiers, however, a core motivation is relatively simple: for money."* (Keller, 2018).

Career satisfaction is accepted as an indicator of subjective career success (Colakoglu, 2011). Because objective career success involves visible results, it is often based on a third person perspective and therefore does not reflect an employee's own assessment of success. In this respect, subjective career success is taken into account in the evaluation of career satisfaction (Ghaleb).

For most of those who chose the military profession, the importance of this choice for personal development is considered. The results are:

- Very important – 60 %
- Important – 35 %
- Neutral – 3 %
- Somewhat important – 2 %.

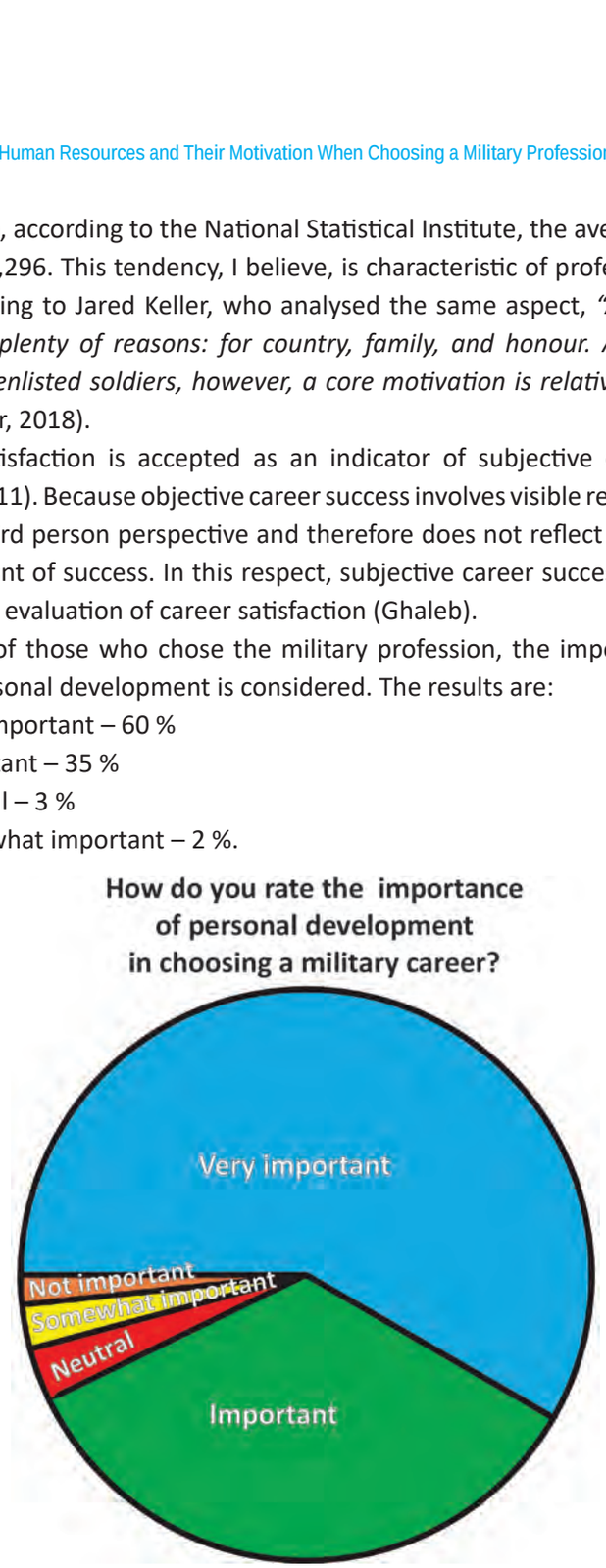


Figure 3 (author's design)

The motivational factors outlined in this way also reveal the value system of the studied young people. They are fully aware of the responsibility of the profession and are ready to serve the country.

CONCLUSIONS

Choosing a profession is a complex and individual process that involves self-understanding, exploring professional options, education and practical experience, as well as career planning. The right approach to each of these aspects can help make an informed and satisfying decision about the career development of each serviceman. Serving one's homeland and preserving peace represent an act of awareness and duty for which those who have chosen military specialties as their profession are ready.

Motivation as a process and motivational factors for the individual in choosing a profession are different for each person. For a person to be successful in his/her profession, he/she needs to be motivated!

But the choice of a military profession is extremely responsible and conscious, because everyone who chooses this profession has sworn to defend the country, to work for peace and the peaceful resolution of regional and global military conflicts! That is why it is necessary for democratic societies and governments to support young people who have chosen military professions, as they bring valuable personal qualities, and the duty to the motherland is in the first place!

Therefore, the benefits of motivation in choosing a profession in a multinational context will increase the quality of human capital, and these benefits are indisputable both for each individual country and for NATO!

BIBLIOGRAPHY:

1. Bakhtyorovich, S.U. (2020). Motivation Problem of the Military Service in *Psychology*, www.idpublications.org/wp-content/uploads/2020/02/Full-Paper-MOTIVATION-PROBLEM-OF-THE-MILITARY-SERVICE-IN-PSYCHOLOGY.pdf, retrieved on 12 July 2024.
2. Funding NATO (2024), https://www.nato.int/cps/en/natohq/topics_67655.htm#direct, retrieved on 26 July 2024.
3. Ghaleb, B.D.S., *The Relationship between Career Selection and Career Satisfaction*, The_Relationship_between_Career_Selection_and_Care.pdf, retrieved on 12 July 2024.
4. Keller, J. (2018). *The Top 5 Reasons Soldiers Really Join The Army, According To Junior Enlisted* (May 14, 2018), https://taskandpurpose.com/5-reasons-soldiers-join-army, retrieved on 15 July 2024.
5. McGregor, D. (1960). *Theory X and Theory Y. Organization Theory,* 358, p. 5.
6. Ministry of Defence of the Republic of Bulgaria, https://www.mod.bg/en/ministry.html, retrieved on 22 July 2024.
7. Доклад за отбрана, https://www.mod.bg/en/ministry.html, retrieved on 12 July 2024.
8. Stefanova, N., https://www.uni-svishtov.bg/portal/getFile/37/Avtoreferat_NS.pdf, retrieved on 12 July 2024.

EFFECTIVENESS OF CIVILIAN OVERSIGHT OF THE SECURITY SECTOR THROUGH PARLIAMENTARY COMMITTEES

Assistant Professor Desislava MADZHAROVA, PhD
University of Library Science and Information Technology, Sofia, Bulgaria
DOI: 10.55535/RMT.2024.4.23

Civil society and parliamentary control over the system for national security are the basic principles of the state system in countries with parliamentary government. Without the observance of basic principles of democratic control, the idea of a democratic and legal state cannot materialize. The complex environment of uncertainty, which includes unconventional-hybrid wars, generates new challenges, risks and threats to national and international security, different from the ones we know. In this context, security sector institutions strive to adapt to the challenges. Since security is central to people's well-being, it is essential that their views should be clearly reflected in the security policy. Parliament is responsible for establishing the legal parameters, adopting the budget and monitoring the relevant activities. To fully exercise these responsibilities, it needs wide access to information, the necessary technical expertise, the power and the intention to keep the executive under control. In this article, we will try to give a real picture of the concept of active citizen control by presenting information analysed and extracted from focus group discussions, which reflects a qualitative and topical nature. The legislative process is a complex factual composition carried out according to a strictly normatively regulated procedure. In this context, the necessity of imposing a legal initiative must be established in advance, based on permanent observations, analytical studies and research. Therefore, the research method used throughout this paper will be that of analytical research.

Keywords: security; Parliamentary control; civil society; sovereignty; hybrid war;

INTRODUCTION: SECURITY IN THE POLICY!

The security of the *polis* is a problem of its citizens. How will it be defended from external attacks is decided by its citizens. The development of social relations, known as democracy, sometimes transformed into an oligarchy, sometimes passing into a tyranny, does not cancel the civil interest in security issues, the crystallization of the internal aspect taking place with Juvenal's question – *"Quis custodiet ipsos custodes?/And who will protect us from the guards?"*.

Obviously, gradually, the leading external security aspect of society begins to coexist with the internal one. Hence the definition of *"civilian control over the armed forces and over activities in the field of national defence is a type of civil activity that is carried out both through the bodies of state power and through free public formations, initiatives and movements of citizens. It is subordinated to the interest, condition and use of the armed forces to meet the interests of society only"* (Rachev, 1996, p. 20). *"L'État, c'est moi/The state, it is me!"* – claimed Louis XIV, the French absolutist king. This quote speaks not so much to the self-evident self-awareness of the divine right of the monarch as to the fact that the claim was controversial even in his days. Almost 75 years after the death of Louis XIV, the French Revolution broke out, the people took over (at least for a short time) the power and the state.

Ideas for civil society:

John Locke

Refusing the state of nature and avoiding the state of war – the main reason for the formation of society. In the *"state of nature"* there is no: generally accepted and recognized law; a knowledgeable and impartial judge; a force ensuring the application of laws and punishing their violators. It justifies the goals and functions of state administration – the protection of the rights and freedoms of citizens and property; formulates the dominant role of the idea of the right of the majority; raises the idea of the right of the people to use force against the government when it tramples by force its own rights.

Jean-Jacques Rousseau

The essence of the legitimate political system consists in the following: a person, uniting with others in a society, to preserve his freedom. Theory of popular sovereignty: source of statehood – the absolute sovereignty of the people; essence – the general will.

FROM TRADITIONAL TO CIVIL SOCIETY

The secularization, i.e. the profanization – the ossification of the social world and of all social relations, the birth and release of private interests, initiative, personal independence, the actual liberation of the previously suppressed natural elements of man etc. pose very acutely the problem of social order, of the conditions of the very existence of society. The state as a mechanism is the solution to the question of civil peace. The state represents a contract between people to establish and preserve social order.

Civil society is a substantial reality, while the state is an instrument of civil society. It is in the viscera of this society that ideas about the desired state crystallize, the general will of the people, the general interests, needs, and goals of society are formed. The forms of civil life are characterized by their self-regulation and self-governance. Self-regulation is carried out with the help of rationalized rules and prescriptions, accepted moral norms, cultural patterns, customs, traditions etc.

Pluralism, which expresses and is based on the differences between people and groups of people, does not contradict unity and the principle of social harmony and social peace. There is a clear need, expressed in society, for the elected representatives of the people in parliament to work closely with the government and the security sector in particular. Although they work towards the same goals, their roles are and should be radically different. The Parliament is responsible for establishing the legal parameters, for adopting the budget and monitoring the relevant activities carried out by the governments. It can fully exercise these responsibilities if it has wide access to information, the necessary technical expertise, the power and the drive to keep the executive under strict accountability and control. Of course, it requires a social structure based on trust and dialogue. Civil society can join this dialogue, it has this right in several ways. Perhaps the best is through non-governmental organizations (NGO) that have a wide range of activities, expertise, financial security and civic initiative. They play a key role in implementing the principles of democratic participation.

The relationship between NGOs and ruling groups has improved over the years in rule-of-law states, which cannot be boasted in societies ruled by authoritarian, totalitarian and undemocratic authorities. In Bulgaria, there is a tendency towards consolidation, mutual trust and cooperation between individual NGOs and the authorities. We hope that a vigilant civil society and the representatives of the people will increase their efforts to ensure that all actors in the security sphere will direct their mutual efforts for the common good of all citizens. The very nature and dynamics of the security sector challenge parliamentary scrutiny itself.

The variety of issues, often technical, the complex organization of people in the sector and reference to secrecy laws, rules and practices make it somewhat difficult for parliamentarians, especially if they do not use independent research or expertise. The idea of control or power is central to the concept of democracy, a concept that may be differently understood or interpreted.

Democratic control refers to the norms and standards governing the relationship between the public and the representative power in the form of the parliament and the democratically elected power subject to supervision by the judiciary, the media and civil society organizations. How does democratic control relate to other concepts affecting the relationship between the security sector and society? Citizen monitoring and control in local self-government is an absolutely necessary element of a democratic state and is an important form of citizen participation in local self-government. It is an essential factor in protecting the rights of citizens and their legitimate interests as well as the well-being of the local community the involvement of interested parties is one of the ways that guarantees the quality of services, being the main mechanism for countering corrupt practices.

In Bulgarian legislation, the public control of the activities of local self-government and local administration is not legally regulated. It is implemented on the basis of the constitutional right of citizens to associate. There are no legal mechanisms regulating the cancellation, amendments or suspension of acts of the local self-government bodies, or removal and monitor legal responsibility of the bodies and officials of the local administration. It is widely believed that security policy is a *"natural"* task for the executive that has the necessary knowledge and can make quick decisions. Parliament is generally considered to be the less appropriate institution when it comes to dealing with security issues, especially with the longer procedures and lack of full information and expertise on the important issues. But at the same time, the parliament is charged with evaluating and monitoring the executive. The political philosophy for determining the place of special services in the security system is laid down in the constitutional text. If there is a place to start, it is the fundamental law itself. Mention should be made, in this context, that civil and human rights are often mistaken, with no clear difference between them. Many times, these two areas are intertwined.

What Are the Possibilities of Exerting Control over the Security Services?

Parliamentary control is a prerequisite for democratic legitimacy. Recent changes in the legislative process and the increased legislative role of the executive have created the need to strengthen parliamentary control procedures. This phenomenon is not alien to the institutional structure, as the main tools

of parliamentary democracy are related to people's vote. The important rule here is that colleagues cannot control colleagues. It is thus proper for parliamentary committees to include deputies professionally removed from both security services and security services. Control is civil in the deepest sense of the term.

The difficulty here comes from the major changes in the composition of the parliament and the need in each new mandate to look for people who have already gained experience as MPs in this area. In democratic societies, the government and parliament, together with the judiciary, share responsibility for the proper functioning of the security sector.

Together they are responsible for the continuous cycle including: formulation of national security and defence policies; enforcing these policies; regular performance reviews and audits. In the allocation of responsibilities, the executive exercises day-to-day control over the implementation of policy in practice. Civilian control of defence and armed forces, to be effective, requires a good understanding of defence and force planning principles, comprehensive, clear and auditable planning procedures, solid citizen participation and strict citizen oversight at every stage of planning. A good working model of civil-military interaction in defence and force planning should be based on:

- Goal-oriented, not necessarily rule-abiding, civil-military cooperation at a working – expert level, where participation is commensurate with the available expertise and specific experience of the participants in the planning process;
- Distribution of decision-making powers depending on specific expertise and personal interest;
- Clear civilian control over defence policy and planning, including authorization of all milestone decisions by the relevant civilian authority.

Parliament's role in developing new national security policy is limited, as this is primarily a government prerogative. However, an important role for parliament is to make the process transparent to the public and thus exerting an indirect influence on policy formation. Parliamentarians must also argue the case for emerging security concepts, must explain why change is needed, and win public support and understanding.

Parliamentary committees provide subject matter expertise and are often consulted in the earlier stages of policy development, when a project is being drafted or time is allowed for reflection and consideration. Committees also use discourse to inform the development of related legal norms. The second phase begins with the formal arrival of an amendment proposal. Especially when defences

are built, committees reject or propose changes to draft documents, the proactive and decisive role of the legislature in the decision-making process becoming visible. The passing of defence legislation and the approval of security policies by parliament are actions considered the most important factors in democratic civilian control, as they must represent the broad sections of the people.

The issue of transparency and accountability is on full display when it comes to monitoring and auditing public spending and government financial requirements. The tools and mechanisms used by parliament to control policy implementation and oversee fund administration are common to most democratic systems and typically include parliamentary debates, questions and interpellations, and parliamentary polls as a means of obtaining information from the executive. Because security is of primary importance to people's well-being, it is essential that their views are clearly reflected in security policy. Parliament is responsible for establishing the legal parameters, adopting the budget and monitoring the relevant activities. It can fully exercise these responsibilities if it has wide access to information, the necessary technical expertise, the power and intent to keep the executive in check. It is achieved by fulfilling several sub-criteria – effective participation, i.e. a real opportunity for each member to bring their views to the attention of other members of the community; voting equality enlightened understanding, i.e. within a reasonable period of time everyone has the opportunity to become familiar with the planned policies and their alternatives and consequences and to form an opinion; control over the agenda, i.e. everyone has an equal opportunity to determine and decide which issues will be included in the agenda; inclusion of the adult population.

Another common ground for democratic societies in the exercise of oversight is the establishment of specialized defence committees and sometimes intelligence committees to oversee government policies and to scrutinize the operations and performance of security sector organizations in this area. The size and special focus of the committees allow for more careful consideration of subjects and offer a better opportunity to reach compromises or find consensus among different political parties on important security issues. In this sense, committees are most influential in preparing new legislation or amendments, also providing expertise and advice on executive projects or petitions before they are brought to Parliament for full debate Committee reports provide guidance to legislators regarding their discussions and their final decisions on issues.

Security clearances for parliamentarians serving on defence committees allow them to hold isolated hearings when secrecy is required, but, beyond the borders

of national security committee representatives, also provide the basic level of transparency to society and the public. All procedures and mechanisms built into constitutional provisions and law to promote accountability of the executive to the legislature and bind both to constitutional principles are not ends in themselves. They serve the general purpose of providing the nation with the most effective security policies that contribute to the best interest of society while striking a balance between the need for security and the maintenance of democratic freedoms and civil liberties. Parliamentary and public control of the budget often clashes with long established executive power in the security sector. However, it can and should be exercised to ensure accountability in the use of public security and defence resources.

The most important role of parliament and parliamentary committees to be effective is to establish an appropriate legislative framework that ensures – as far as possible within the particular constitutional framework – the application of all principles and legislation for a comprehensive audit and control process. Apart from it, parliamentary and public oversight of the security sector through the budget must be firmly rooted in the country's political culture.

INSTEAD OF CONCLUSIONS

Civil control in state administration is an absolutely necessary element of any democratic state. It is an essential factor for protecting the rights of citizens and their legitimate interests. The involvement of interested parties is one of the ways that guarantees the quality of services, as well as the main mechanism for countering corrupt practices. When developing a new policy or considering a change to an existing one, the process should be open to all stakeholders, but mechanisms and procedures should be used to take into account the views and opinions of those who would be affected or those who have a particular interest in the particular policy or change thereof. In Article 21 of the Law on the Management and Functioning of the System for the Protection of National Security, it is stated that *"the activities of the bodies and structures of the system for the protection of national security shall be subject to parliamentary, administrative, judicial and civil control"*. The principles of good governance require the active participation and cooperation of the various partners – state institutions, local authorities, citizens and structures of civil society, in formulating, implementing and controlling the various policies. The dialogue between the local government and the interested parties is an important part of the process of development, implementation and monitoring of the national security policy in the Republic of Bulgaria. The processes of civil

participation in the monitoring and control over the implementation of policies can be mandatory, i.e. required by law, and optional – initiated by the will of the local administration or the local public. In order for society to be more active and transparent in its exercise of civil control, there should be active participation and dialogue:

- Participation in cross-sectoral working groups;
- Participation in expert meetings, forums and information campaigns;
- Participation in information meetings, round tables, conferences, seminars and others;
- Participation in polls and public opinion research.

As a full member of the EU, in relation to the role of national parliaments in the democratic control of European security and defence, it should be noted that there is diversity and difference in the procedures of individual member states, Bulgaria included. However, the basic conditions on which this process takes place can be structured into several groups.

First of all, the existence of special legislation in some countries that regulates the conduct of military operations and civilian missions – the conditions for participation, the procedures and the main institutions, thus creating a clear normative basis for CSDP decision-making. In some countries, this process is not explicitly regulated in the legislation, but nevertheless the permanent practice has required the government representatives to conduct preliminary consultations and require the sanction of the parliament.

The exchange of information through hearings in the plenary hall and at meetings of departmental committees should be indicated as a further instrument for control of national parliaments. In these cases, the government has an obligation to provide MPs with information and documents regarding the joint actions undertaken within the framework of the European defence policy, as well as the manner of spending funds within the budget intended for defence (from the point of view of effectiveness, efficiency and transparency).

An important role in this process is played by the relevant committees of national parliaments, namely the security and defence committees. Regarding the European Parliament (EP), it should be emphasized that the control exercised by the EP over the common security and defence policy in no way replaces or hinders that of national parliaments.

The ability to finance certain operations within the security and defence policy with funds generated from the Community budget predetermines the control powers of the EP. The European Parliament has the right to organize public hearings

on current issues of security and defence policy, at which the financial aspects of the operations, the decision-making process and the assessment of the progress achieved and the challenges ahead are discussed.

Forms of interaction between national parliaments and the EP on security and defence issues with additional democratic control over policies in the security and defence sector are also implemented through the interparliamentary dialogue.

First of all, the Treaty of Amsterdam created a Conference of Committees on European Affairs, which is a forum for discussions in which representatives of national parliaments from the departmental committees on European affairs meet, as well as members of the European Parliament. The European and national parliaments are also represented within the NATO Parliamentary Assembly, which contributes to deeper analysis and cooperation between the two organizations on security and defence issues.

The gradual strengthening of the integration processes in the sphere of European security and defence is invariably related to assuming new responsibilities and contributing to the resolution of individual regional problems or crises.

The successful inclusion of the EU in this framework is tied to strengthening the accountability and democratic control of the sector. Parliamentary control in the security and defence sector with a view to striving for more effective public diplomacy and legitimization of actions in the security and defence sector, the new powers of the national and European parliaments, after the Lisbon Treaty, the control over the spending of funds for participation in civil and military missions, as well as the idea launched in the present development of the European Semester of defence should be also presented. The world has not become a more peaceful place even after the end of the *"Cold War"*, and even less so in recent years. What is happening in the security environment confirms the need to strengthen the power of the state – military, political, economic, civil and informational, in the name of stability, security, a healthy nation.

The ongoing Strategic Review of the system for the protection of national security and Strategic Review of Defence should clearly show what defence capabilities Bulgaria should have, to continue the modernization and strengthening of the defence. It will be very useful to reach a consensus because it will give stability on the main priorities of the defence policy and the policy in the security sector in the medium and long term.

BIBLIOGRAPHICAL REFERENCES:

1. Andersen, L. (2006). *Security Sector Reform in Fragile States*. Copenhagen: Danish Institute for International Studies Working Paper No. 15.

2. Born, H and Fluri, P. (2003). *Oversight and Guidance: The Relevance of Parliamentary Oversight for Security Sector Reform*. Geneva: Centre for the Democratic Control of the Armed Forces Working Paper.
3. Born, H., Fluri, P., Johnsson, A. (eds.) (2003). *Handbook for Parliamentarians* No. 5, Parliamentary Oversight of the Security Sector: Principles, Mechanisms and Practices. Geneva: Inter-parliamentary Union and Centre for the Democratic Control of the Armed Forces.
4. Caiden, G.E., MacDermot, N., Sandler, A. (1983). *The Institution of Ombudsman*. In Caiden, G.E. (ed.). International Handbook of the Ombudsman. Westport, Connecticut: Greenwood Press.
5. Centre for Human Rights. (1995). *National Human Rights Institutions: A Handbook on the Establishment and Strengthening of National Institutions for the Promotion and Protection of Human Rights*. Geneva: United Nations Professional Training Series No. 4.
6. United Nations Development Programme. (2002). *Human Development Report 2002: Deepening Democracy in a Fragmented World*. New York: Oxford University Press.
7. Juvenal's question, https://bg.wikiquote.org/wiki/%D0%AE%D0%B2%D0%B5%D0%BD%D0%B0%D0%BB, retrieved on 7 August 2024.
8. Rachev V. (1996). *Security and armed forces in a democratic society: basic issues of leadership and control*. In Pantev P., Rachev, V., Tagarev, T. *Problems of civil-military relations in Bulgaria. Approaches to improving civilian control over the armed forces*, Research Studies-2, IISMO, Sofia, 1996, p. 20.
9. Sung Ho Kim (2004) *Max Weber's Politics of Civil Society*, Cambridge University Press.

ENERGY RESILIENCE DURING ARMED CONFLICT: RECONSIDERING HYDROGEN FOR EUROPEAN UNION ENERGY SECURITY

Marinela-Luminița Emanuela ZLATEA, PhD Student

Department of International Business and Economics, Academy of Economic Studies, Bucharest

Professor Alexandra-Lavinia HOROBEȚ, PhD

Department of International Business and Economics, Academy of Economic Studies, Bucharest

Eugen Constantin ROȘCA, PhD Student

Doctoral School, Faculty of Economic Studies, "Lucian Blaga" University, Sibiu

DOI: 10.55535/RMT.2024.4.24

The Russian-Ukrainian war has raised concerns about the security of energy supply, prompting Europe to make changes in its energy mix. With the launch of REPowerEU, the EU aims to transition as quickly as possible from dependence on Russian fossil fuels to increased energy autonomy and clean energy production. Accelerating renewable hydrogen production by 2030 is part of this plan.

The present study uses clustering algorithms to assess the action capacity of the European Union countries regarding hydrogen perspective, by considering hydrogen production and infrastructure projects. The war has accelerated the transition to clean energy sources and energy independence, which is reflected in the reduction of CO2 emissions and the increased interest of member state governments and private entities in issuing green bonds. Investments in green hydrogen can boost economic growth and resilience but require the creation of a functioning market and a flexible regulatory framework.

Keywords: energy security; hydrogen; war; renewable energy; European Union;

INTRODUCTION

The Russian-Ukrainian war, which began in February 2022, has profoundly affected global energy dynamics, bringing to the fore the energy independence, and accelerating the transition to renewable energy sources. In response to the energy market imbalance, the European Commission launched the *REpowerEU Plan* in May 2022, an initiative aimed at phasing out energy imports from Russia and the significant green energy intensification (European Commission, 2022-a). Green hydrogen is an important component of REpowerEU, with estimated total imports and production of around 20 million tonnes by 2030 (European Commission, 2022-b). The plan also includes measures to support the development of hydrogen infrastructure and markets, so that green hydrogen can be produced, transported, and used efficiently in different sectors. However, since the drafting of the *EU Hydrogen Strategy*, opportunities arose regarding its role in the storage of renewable energy and in the reduction of CO2 emissions among certain sectors such as the steel, chemical and transport sectors (European Commission, 2020-a). The strategy aims to develop a European hydrogen economy, by creating new economic opportunities and stimulating the growth of the EU's competitiveness, with focus on research and innovation, which are essential for achieving these goals.

Resulting from the process of water electrolysis, green hydrogen has gained significant interest in the transition to a more sustainable energy system, being considered a potential clean energy solution because it is produced using renewable energy sources such as solar or wind energy. More and more countries have begun to pledge climate neutrality and look for solutions to reduce CO2 emissions, thus investments to stimulate the production and use of green hydrogen have substantially increased in recent years. Recently, approximately €6.9 billion (US$7.4 billion) has been allocated at the EU level for green hydrogen production projects under the *Important Projects of Common European Interest (IPCEI)* initiative (Hydrogen Insight, 2024-a). The EU has also approved €998 million (about US$1.1 billion) in state aid for renewable hydrogen production in Netherlands (Hydrogen Insight, 2024-b). To create investment security and business opportunities for both European and global production of hydrogen from renewable sources, the European Commission launched the European Hydrogen Bank (EHB) in 2022. The first EU-wide auction under the EHB awarded almost €720 million to seven renewable hydrogen projects

in Europe and it is expected to produce around 1.58 million tonnes of renewable hydrogen over the next ten years (European Commission, 2022-c).

The EU's efforts to build its own energy fortress while maintaining climate neutrality are numerous, but what happens when geopolitical changes occur? How has the war between Russia and Ukraine changed global energy dynamics and renewable energy discourse? Additionally, how can the EU, given the current context, align energy security with climate goals? Our research aims to fill this gap and analyse how the Russian-Ukrainian war brings to the fore the importance of green hydrogen as an alternative for EU goals. We check out the European green hydrogen market from the launch of the *EU Hydrogen Strategy 2020* until now. We consider variables of interest such as hydrogen consumption and supply, hydrogen infrastructure and production projects, to identify similarities and differences between EU countries from the perspective of hydrogen economy development. The variables are complemented by green bond issuance by corporates and governments, the share of renewable energy in gross final energy consumption and net greenhouse gas emissions, which show these countries' progress in the energy transition. Thus, in the first part of the paper we analyse the main results obtained in the literature on green hydrogen research, so that in the second part we describe our research methodology and results. In conclusion, we highlight the most important ideas and limitations of the paper, to which we add some potential themes for future research.

LITERATURE REVIEW

The biggest challenge in producing clean hydrogen is the energy source utilised. The desirable framework to meet both climate neutrality and energy security goals is for green hydrogen to be produced using entirely renewable sources. Thus, the whole process does not require the depletion of natural resources and does not involve CO2 emissions. Moreover, the production of green hydrogen can create a sustainable energy system, thereby harnessing renewable energy sources and helping to reduce dependence on fossil fuels. However, the high cost of renewable energy technologies and the need for significant development of storage and distribution infrastructure represent a challenge.

The specialized literature focuses mainly on this issue. There are numerous studies that have attempted to classify hydrogen according to the type of technology used in its production. Pilavachi et al. al (2009) analysed seven common hydrogen production processes, depending on different types of cost and CO2 emissions,

respectively: steam methane reforming (SMR), partial oxidation of hydrocarbons (POX), coal gasification (CG), biomass gasification (BG), photovoltaic-electrolysis system (PV-EL), wind-electrolysis system (W-EL) and hydropower-electrolysis system (H-EL). Their results demonstrated that, in most cases, the processes that combine renewable energy sources with electrolysis were considered to be better than conventional processes, with the hydropower-electrolysis system ranking first in the production process, and coal gasification at the opposite pole (Ib., p. 9). *EU Hydrogen Strategy* classifies it according to the technology and energy source used into the process: electricity-based hydrogen, renewable hydrogen, clean hydrogen, fossil fuel-based hydrogen, fossil fuel-based hydrogen with carbon capture, low-CO2 hydrogen, and hydrogenated synthetic fuels. The Commission's communication noted that *"neither renewable hydrogen nor low-carbon hydrogen, particularly fossil fuel-based hydrogen with carbon capture, is cost-competitive with carbon-based hydrogen fossil fuels"* (European Commission, 2020-b, p. 5).

For a better classification of hydrogen types, the International Renewable Energy Agency (IRENA) has proposed a nomenclature of colour codes for each type, depending on the energy source used: grey (produced from fossil fuels, more precisely steam methane reforming – SMR or coal gasification), blue (grey hydrogen, but with carbon capture technologies – CCS)), turquoise (combines the use of natural gas as a raw material, without the production of CO2; thus, through the pyrolysis process, the carbon from methane becomes solid black carbon) and green (water electrolysis powered by electricity from renewable energy sources) (IRENA, 2020, p. 9).

There have also been specialized studies that have made technical and economic comparisons between hydrogen production technologies to understand their feasibility. Thus, other colours have been added such as: aqua, brown or black, white, yellow, pink or purple and red (Ji, Wang, 2021; Ajanovic et al., 2022; Arcos, Santos, 2023; Dash et al., 2023). Ji and Wang (2021) demonstrated that, in the short term, SMR remains the dominant technology due to its maturity, and CG may be more applicable in some regions due to the local distribution of resources. But to change this status quo, one option is to combine carbon capture technology to control CO2 emissions, which is less feasible given the limited reserves of fossil fuels. The second option is the gradual transition to green hydrogen production, with electrolysis and thermochemical methods, demonstrating considerable development potential from an economic and ecological point of view (Ji, Wang, p. 18). Arcos and Santos (2023) showed that green hydrogen remains the most expensive of all other

types, followed by purple or pink hydrogen (obtained by nuclear power), and aqua hydrogen (derived from oil sands extraction, natural bitumen, and conventional oil fields) is the cheapest, but it must be emphasized that this type of hydrogen is still at an early stage and has not been adequately tested. Each method of producing hydrogen has different factors that must be considered. The composition of the energy mix, for example, determines the amount of CO2 emissions generated. Therefore, although technologies with significant GHG emissions currently have the highest levels of maturity and lower costs, it is important that they are phased out and low-carbon production methods must continue to evolve and improve to achieve low cost and no GHG emissions. (Arcos, Santos, p. 15).

In the context of the war against Ukraine, energy researchers have mainly focused on issues related to transport infrastructure, supply chain and cooperation with different countries to ensure hydrogen partnerships.

Transport infrastructure is a critical component for the development of the hydrogen economy. Although it could be seen as a long-term goal, it was trying to find some short-term solutions. An alternative intensively researched by specialists is the use of the current gas infrastructure and the mixing of hydrogen in the natural gas network. Vadaszi et al. (2023) found that hydrogen can be directly blended in the distribution network, transported through the natural gas system, and stored in underground gas storages, but it must be considered that the implementation method differs from country to country depending on the existing infrastructure, the available legal framework, and the specific geological conditions. Their study proposes as a strategy the interconnection of the gas and electricity sectors and the increase of biogas production. Thus, if there is a surplus in the electricity system due to intensive renewable energy generation, then hydrogen can be produced with the excess energy and transported through the existing infrastructure. The conclusions highlight that the replacement of natural gas with 100% hydrogen remains only at a theoretical level for now, requiring a special infrastructure and technology (Vadaszi et al., p. 3). Bin Jumah (2024) showed that it is essential to improve the energy density of hydrogen to make its transport and storage possible, but specialized infrastructure is needed, which requires additional costs for processes such as compression, liquefaction, or the use of chemical carriers (bin Jumah, p. 18). The question was raised including the production of hydrogen in eco-industrial parks (EIP), which involve the creation of a cluster of industrial and commercial activities with the aim of minimizing waste and optimizing the use of resources. Eco-industrial parks can provide the necessary infrastructure for hydrogen

production and distribution and reduce production, transport, and distribution costs, thereby creating economies of scale (Reda et al., 2024, p. 15).

But hydrogen storage is not only determined by storage tools or transport infrastructure, but also by the evolution of supply and demand, as well as the interaction with other sectors. Münster et al. (2024) showed that the decrease in demand for natural gas led to an increase in the short-term demand for hydrogen. In the long term, the availability of green and blue hydrogen increases the demand for hydrogen imports, which can impact the necessary infrastructures. According to their study, the limited availability or high price of natural gas, accompanied by a high demand for hydrogen can increase the production of green hydrogen. Also, rising natural gas prices affect the cost of blue hydrogen, while rising electricity prices affect the cost of green hydrogen, thus there are cost variances due to uniform natural gas prices versus electricity prices (Münster et al., p. 22). Erdoğan and Güler (2023) projected the hydrogen supply chain for hydrogen fuel cell electric vehicles (HFCEV) in Türkiye over a 25-year period (2026–2050). Low demand and high capital cost lead to an increase in the unit cost of hydrogen until 2031 but will reach the lowest values by 2050 due to the supply chain maturation. Their study considers the best strategy to be mixed production, based on SMR (cost oriented) on the one hand, and on electrolysis (oriented to zero CO2 emissions), on the other hand (Erdoğan, Güler, p. 13).

The potential of green hydrogen relies also on geographical location and abundant natural resources. In August 2020, Germany and Ukraine launched an energy partnership that includes the development of a hydrogen-based economy. Ukraine has vast renewable energy resources that can contribute to the production of *"green"* hydrogen, as well as a gas transportation system useful for hydrogen distribution. For this, it is necessary to accelerate the development of the regulatory framework in Ukraine and harmonize it with Germany, considering the already existing norms and obligations of Ukraine in the field (Hritsyshyna, Hutarevych, 2021, p. 21). The regulatory framework also remains a challenge for the EU-Morocco partnership on hydrogen production, but it is not a major barrier like market readiness, water shortages and territorial disputes in Morocco.

We therefore consider the analysis of renewable energy sources in the EU that can contribute to the production of green hydrogen, taking into account the potential transport infrastructure, as well as the potential clean hydrogen demand and supply.

METHODOLOGY

Starting from the results obtained in the literature, we propose to analyse the potential of hydrogen in the EU-27 regarding the transition to green energy, given the armed conflict in Ukraine. *Table 1* includes variables description.

Table 1: Variables description

Acronym	Variable	Period	Unit of measure	Source
GRB	Green bond issuance by corporates and governments	2022	% of total	Eurostat
REN	Share of renewable energy in gross final energy consumption	average 2019-2022	%	Eurostat
GES	Net greenhouse gas emissions	average 2019-2022	tonnes per capita	Eurostat
H2IP	Hydrogen Infrastructure Projects	NA	no. of projects	European Hydrogen Observatory
H2PP	Hydrogen Production Projects	NA	no. of projects	European Hydrogen Observatory
H2TC	Hydrogen - Total Consumption	average 2019-2024	thousand metric tons oil equivalent	S&P Energy Portal
H2TS	Hydrogen - Total Supply	average 2019-2024	thousand metric tons oil equivalent	S&P Energy Portal

The research utilized clustering methods to examine the similarities and disparities among EU countries in relation to their hydrogen development. Three principal *clustering methodologies* were employed: *hierarchical clustering* (also known as joining or tree clustering), *k-means clustering*, and *two-way joining*. These methodologies were selected for their capacity to discern patterns

and categorize countries according to various characteristics associated with hydrogen development. The level of countries' progress in producing and using hydrogen was captured by 4 variables:

(1) Hydrogen Infrastructure Projects – H2IP;

(2) Hydrogen Production Projects – H2PP;

(3) Hydrogen – Total Consumption, average 2019-2024 (thousand metric tons oil equivalent) – H2TC;

(4) Hydrogen – Total Supply, average 2019-2024 (thousand metric tons oil equivalent) – H2TS.

To them, we added 3 more variables that describe EU countries' net greenhouse gas emissions, as an average 2019-2022 (in tonnes per capita) – GES, as well as their progress in the green transition: REN – Share of renewable energy in gross final energy consumption, average 2019-2022 (%), and GBR – Green bond issuance by corporates and governments, 2022 (% of total). Data was collected from Eurostat, European Hydrogen Observatory and S&P Energy Portal, for all 27 EU countries between 2019 and 2024, depending on availability.

The *hierarchical clustering*, employing Ward's amalgamation method and Euclidean distances, generated a dendrogram that visually depicts the links across countries (Murtagh, Legendre, 2014). This method facilitated the recognition of embedded clusters without predefining their number. *K-means clustering*, an iterative partitioning technique, was subsequently employed to form distinct, non-overlapping groupings of countries exhibiting analogous hydrogen development trajectories (Jain, 2010). The number of clusters was established through the elbow approach and silhouette analysis to enhance intra-cluster similarity and inter-cluster dissimilarity. A *bi-clustering technique* known as two-way joining was utilized to concurrently cluster countries and variables, uncovering correlations between distinct subsets of countries and specific dimensions of hydrogen development, also in relation to countries' progress in the energy transition (Madeira, Oliveira, 2004). The application of Euclidean distances across all three methods guarantees uniformity in assessing the similarity among data points. Ward's approach, utilized in *hierarchical clustering*, minimizes within-cluster variance, resulting in compact and distinctly differentiated clusters (Murtagh, Legendre, ib.). The integration of various clustering methodologies established a comprehensive framework for discerning leaders, followers, and prospective partnership prospects within the European hydrogen sector.

RESEARCH RESULTS

In order to distribute the analysed countries in groups as homogeneous as possible, but differentiated from one cluster to another, two clustering algorithms were applied: the *iterative algorithm (Figure 1)* and the *k-means clustering (Figure 2)*. All variables were standardized to remove the impact of different measurement units and were introduced into the algorithm using Tibco Statistica.

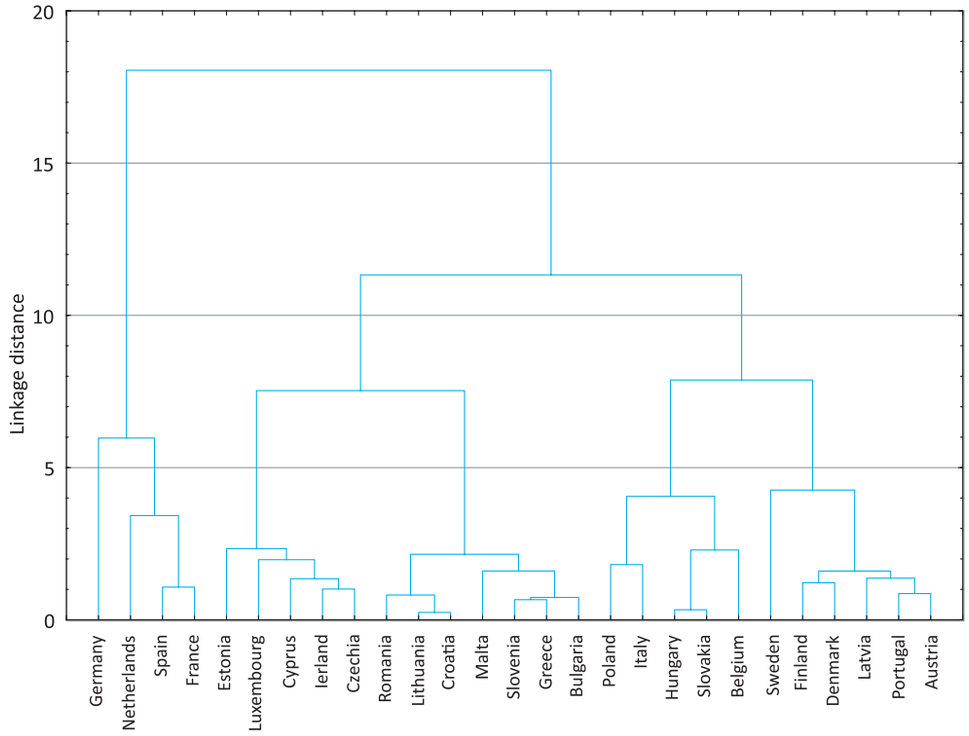


Figure 1. The dendrogram – hierarchical clustering
(authors' calculations and representations in Tibco Statistica)

Figure 1 presents the results obtained from applying the *iterative algorithm*. The horizontal axis contains the number of identified clusters and the countries that are part of these clusters, and the distance between the cluster centres is shown on the vertical axis. Thus, 2 clusters of countries were obtained: Germany, the Netherlands, Spain, and France (Cluster 1) and the rest of the EU-27 countries (Cluster 2). Cluster 1 contains countries with specific particularities in terms of renewable energy and especially the production and use of hydrogen, compared to the countries in cluster 2. Germany, the Netherlands, Spain, and France are among the top countries in terms of both resources of renewable energy and significant

investments and hydrogen production capacity. Together with Poland, Italy, the UK, and Belgium, they together account for 74% of Europe's total hydrogen production capacity. (European Hydrogen Observatory, 2023, p. 12). In our analysis, Poland and Italy show similar characteristics and belong to cluster 2.

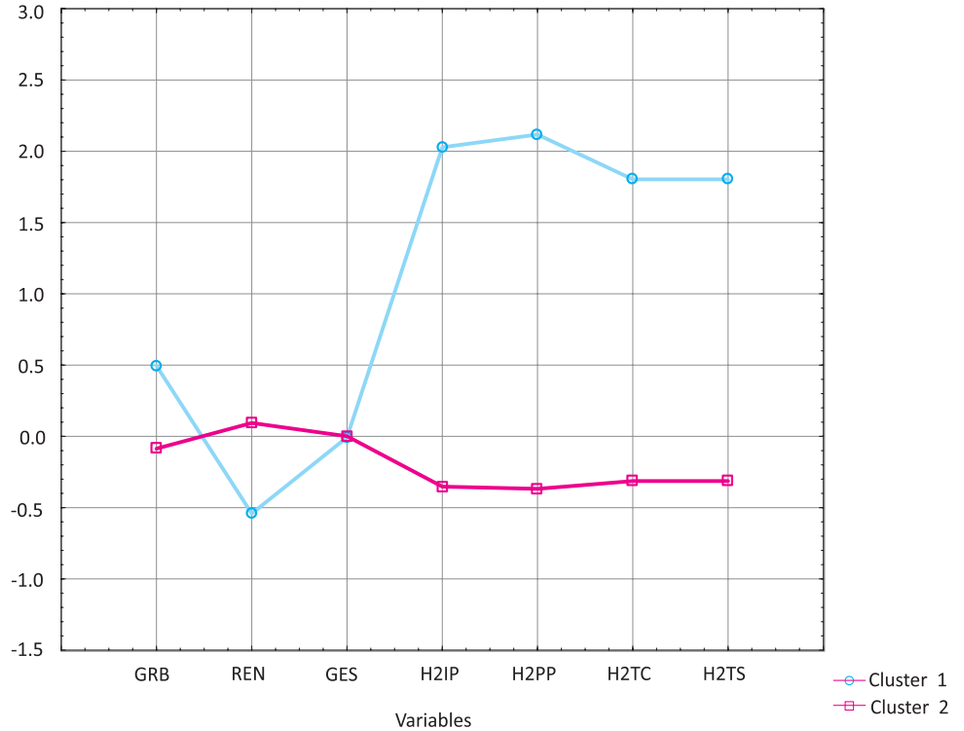


Figure 2. The k-means clustering (Ib.)

Figure 2 shows the normalized means for the two clusters. Cluster 1 is superior to cluster 2 in all variables except for REN, and equal in GES, but for all hydrogen variables, cluster 1 is clearly at a much higher level than cluster 2. The result is surprising regarding the share of renewable energy in gross final energy consumption for cluster 1 countries, but when we consider the hydrogen variables, we associate the share of renewable energy resources in hydrogen production. 91% of the total hydrogen production capacity comes from natural gas reforming or coal gasification. In contrast, clean methods such as reforming with simultaneous carbon capture and water electrolysis production have a minor contribution – less than 1% of the total hydrogen production capacity (Ib., p. 15). The GES variable is similar for both clusters, suggesting that EU countries have aligned with climate neutrality directives and made significant progress in reducing greenhouse gas

emissions. This variable is therefore not significant from the perspective of grouping EU countries into the two clusters.

When looking at green bond issuance by corporations and governments, we see no significant difference between the two clusters. In addition, the level is also slightly close to the GES variable for both clusters, which could mean that together with the EU's climate neutrality objectives, the interest of member state governments and private entities in issuing green bonds has also increased. Green bonds help finance the assets needed for the transition to a low-carbon economy. Thus, in 2023 the European Green Bond Standard (EUGBS) entered into force with the aim of establishing a clear and transparent framework, as well as improving the impact of green bonds at EU level (European Commission, 2023).

Regarding hydrogen production and infrastructure projects, *k-means clustering* results show that states in cluster 1 are clearly superior to states in cluster 2 *(figure 2)*. This can be seen through the massive investments they are making in hydrogen projects. Following European Commission approval in February 2024, the German government has awarded €4.6 billion to 23 green hydrogen projects under *Hy2Infra*. With these, Germany provides up to 1.4 GW of hydrogen production capacity powered by renewable energy, up to 370 GWh of storage solutions and 2000 km of hydrogen infrastructure (Hydrogen Insight, 2024-c). The Netherlands is also making great progress in green hydrogen production. Groenvermogen NL's new project, *HyPRO*, is the largest green hydrogen research and development project in the Netherlands to date and focuses on improving electrolysis technology to reduce the cost and increase the production of green hydrogen (Hydrogen Central, 2024). As early as 2020, when the *National Hydrogen Strategy* was published, France aimed to become a leader in green hydrogen, with the ambitious goal of creating an installed electrolyser capacity of 6.5 GW by 2030, capable of producing 680,000 tonnes of renewable hydrogen every year (France Hydrogène, 2023). In 2022, as part of the *Important Project of Common European Interest*, the European Commission selected 15 French initiatives, among them: the Belfort electrolyser factory (with McPhy), the hydrogen production plant in Dunkirk (with Air Liquide) and the research project and H2 mobility development in Flins-sur-Seine (Hyvia – Renault Group and Plug Power) (H2 Energy News, 2022). The Spanish energy company Enagás is also part of the *European Commission's Projects of Common Interest*, which estimates a renewable hydrogen production of approximately 2.5 million tons per year in 2030. The Spanish infrastructure projects will be connected to the future H2Med corridor, through which Enagás aspires to transform

the Iberian Peninsula into Europe's main hydrogen hub. This corridor also includes the section between Celorico da Beira in Portugal and Zamora (CelZa) and the maritime connection between Barcelona and Marseille (BarMar). This pipeline will be essential for Spain to be able to export its energy surpluses, thereby helping to achieve Europe's goal of producing around 10 million tonnes a year of the 20 million tonnes expected to be consumed by 2030 (Invest in Spain, 2024).

The hydrogen consumption and supply variables are also high for cluster 1 compared to cluster 2. The consumption level of countries in cluster 1 is also high, similar to the production level. Germany (21%), the Netherlands (12%), and Spain (7%) account for almost 50% of Europe's combined hydrogen demand (4.12 Mt/year). In contrast, most European countries show relatively modest hydrogen consumption – less than 10% of each country's total hydrogen demand (European Hydrogen Observatory, 2023, p. 44). The similar level of the two variables indicates that for each country, regardless of the cluster, the current domestic production fully covers domestic demand/consumption.

The *k-means clustering* algorithm method indicates the optimal number of clusters based on ANOVA testing. *Table 2* shows the distances between the clusters and demonstrates that it is the hydrogen-related variables that discriminate between the two groups of countries. Thus, the larger the distance, the more different the clusters are.

Table 2: ANOVA testing
(authors' calculations and representations in Tibco Statistica)

	Between	df	Within	df	F	p value
GRB	2.016	1	23.984	25	2.101	0.160
REN	1.056	1	24.944	25	1.059	0.313
GES	0.865	1	25.135	25	0.861	0.362
H2IP	18.768	1	7.232	25	64.872	0.000
H2PP	10.625	1	15.375	25	17.277	0.000
H2TC	17.122	1	8.878	25	48.216	0.000
H2TS	17.122	1	8.878	25	48.216	0.000

The hydrogen infrastructure projects (H2IP) variable shows greater heterogeneity between clusters compared to the hydrogen production projects (H2PP) variable. We can associate these results with consortium projects and initiatives that focus on creating hydrogen supply corridors, which increases their importance

at the consortium level and less for each individual country. Also, when we refer to hydrogen infrastructure, we consider distribution and storage infrastructure. Germany, for example, already has a network of over 1,800 kilometres of converted and newly built hydrogen pipelines and is working on developing a central hydrogen network by 2028 (The Federal Government, 2024). Thus, the results coincide with the conclusions of the study by Vadaszi et al. (2023), who found that hydrogen can be transported through the natural gas system and stored in underground storages, but it must be considered that the implementation method is different from country to country, depending on the existing infrastructure, the available legal framework, and specific geological conditions. Conversely, within the cluster, the variable of production projects has a much higher relevance, which may suggest that they have become increasingly interested in starting green hydrogen production projects. It is also supported by the ANOVA results regarding GRB, REN and GES at the intra cluster level. In addition, some countries such as Spain benefit from favourable climatic conditions for the generation of renewable energy (solar, wind etc.) to support the production of green hydrogen.

Figure 3 shows the result of the *two-way joining clustering*, in the form of a heatmap of countries according to the selected variables. Markings with yellow, orange and red show a better positioning of the countries on the respective variables, except for GES, where the better positioning is given by the colours in the green spectrum. Regarding the GRB variable, in 2022 Sweden, Slovakia and Hungary topped the ranking in terms of green bond market, supporting environmental protection projects. Our results are also confirmed by the analysis of the European Environment Agency (2023). Some countries, like Sweden, have been active in the green bond market for several years. In 2013, Gothenburg, from Sweden, became the first city in the world to issue green bonds (SEK 500 million). The proceeds from issued green bonds are used to finance climate change projects that promote the transition to green energy (United Nations, 2023). But the increased interest in financial instruments designed to finance climate change projects has also been fuelled by the war in Ukraine. Although in the short term the war created imbalances in financial markets, in the long term it accelerated the transition to clean energy sources and energy independence, prompting governments and corporations to invest more in renewable energy. In terms of hydrogen consumption and supply, Germany, Netherlands, and Poland remain the main players on the market, results also confirmed by the European Hydrogen Observatory report (2023). Germany, France, and Netherlands take the main places in terms of hydrogen infrastructure projects, and Germany, France and Spain stand out for production projects.

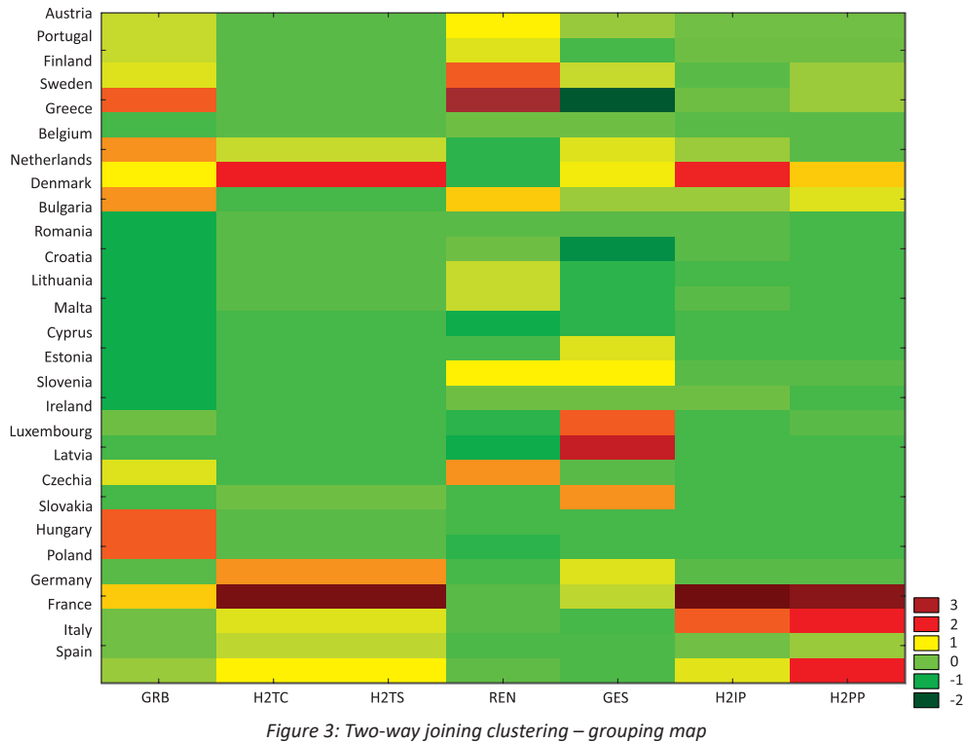


Figure 3: Two-way joining clustering – grouping map
(authors' calculations and representations in Tibco Statistica)

CONCLUSIONS

Our study applied clustering methods to examine similarities and differences among the EU-27 countries in hydrogen development, considering the armed conflict in Ukraine.

Germany, Netherlands, Spain, and France remain the countries with the most significant development in terms of both renewable energy resources substantial investments, and hydrogen production capacity. When we consider the share of renewable energy resources and relating it to hydrogen production, we notice that in these countries, natural gas reforming or coal gasification remains the most used method compared to energy from renewable sources. It may also be due to the local distribution of resources, as demonstrated by Ji and Wang (2021). It is also easy to understand that the electrolysis method is the most expensive of all the other methods due to the high consumption of renewable energy used, but it must continue to evolve and improve to achieve low costs and no GHG (Arcos, Santos, 2023).

In terms of reducing carbon dioxide emissions, our results show that EU-27 countries have aligned with climate neutrality goals and made significant progress towards it, which is also reflected in the increased interest of member state governments and private entities for the issue of green bonds. Although the war created short-term imbalances in financial markets, in the long term it accelerated the transition to clean energy sources and energy independence, prompting governments and corporations to invest more in renewable energy.

Germany, the Netherlands, and Poland are the main players in the market in terms of hydrogen consumption and supply, but the similar level between the two variables for all countries analysed indicates that domestic production fully covers domestic demand/consumption.

Hydrogen infrastructure projects have a greater contribution at the level of country groups, which can be associated with consortium projects and initiatives focusing on creating hydrogen supply corridors, thus increasing their importance at the consortium level and less for each country individually. Also, some countries such as Germany already have distribution and storage infrastructure, including networks built from converted gas pipelines. It complements the results of the study by Vadaszi et al. (2023), which demonstrates that hydrogen can be transported through the natural gas system and stored in underground storage, but it must be considered that the method of implementation differs from country to country, depending on the existing infrastructure, the available legal framework, and specific geological conditions. Conversely, hydrogen production projects are of much greater interest for each country individually, which is also reflected in the reduction of carbon dioxide emissions, as well as the increased interest of member state governments and private entities issuing green bonds. Moreover, some countries such as Spain benefit from favourable climatic conditions for the generation of renewable energy (solar, wind etc.) to support the production of green hydrogen.

The level of interest in projects aimed at the transition to renewable energy is increasing more and more for EU governments, as well as for actors from the private sector. Although expensive, green hydrogen remains the alternative for eliminating dependence on Russian fossil fuels, but also for ensuring energy security from renewable sources, contributing to the goal of climate neutrality. Massive investments and grants for the development of green hydrogen production, infrastructure, distribution, and storage projects demonstrate its importance in meeting current and future energy security challenges.

European states must continue to develop a more resilient and sustainable energy system, considering the geopolitical impact of regional conflicts on energy

security. Thus, the creation of a clear and stable regulatory framework helps to attract investment in green hydrogen and renewable energy, as well as fiscal incentives and subsidies to improve efficiency, investment in distribution networks and storage facilities, and to reduce the costs of green hydrogen technologies.

Our study is limited by the lack of data availability, especially for green hydrogen, given the embryonic stage of the production technology. However, many future research topics remain. Beyond the topics related to hydrogen production, cost, and distribution and storage infrastructure, a first topic of interest could be the expansion of hydrogen in military technologies, but also as an energy resource, given the current context of the conflict in Ukraine. Moreover, it is also necessary to study in detail the transformation of Ukraine into an energy hub, also for hydrogen production, taking into account its renewable resources and infrastructure.

BIBLIOGRAPHICAL REFERENCES:

1. Ajanovic, A., Sayer, M., Haas, R. (2022). *The economics and the environmental benignity of different colors of hydrogen*. In *International Journal of Hydrogen Energy*, 47(57), 24136-24154.
2. Arcos, J.M. M., Santos, D.M. (2023). *The hydrogen color spectrum: techno-economic analysis of the available technologies for hydrogen production. Gases*, 3(1), pp. 25-46.
3. Bin Jumah, A. (2024). *A comprehensive review of production, applications, and the path to a sustainable energy future with hydrogen*. *RSC advances*, 14(36), 26400-26423.
4. European Commission (2023). *The European green bond standard – Supporting the transition*, https://finance.ec.europa.eu/sustainable-finance/tools-and-standards/european-green-bond-standard-supporting-transition_en, retrieved on 16 September 2024.
5. European Commission (2020-a). *Key actions of the EU Hydrogen Strategy*, https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52020DC0301, retrieved on 5 September 2024.
6. Europea Commission (2020-b). *O strategie pentru hidrogen: pentru o Europă neutră climatic*, eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52020DC0301, retrieved on 10 September 2024.
7. European Commission (2022-a), *REPowerEU Plan*, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022SC0230, retrieved on 29 August 2024
8. European Commission (2022-b), *Hydroge*n, https://energy.ec.europa.eu/topics/energy-systems-integration/hydrogen_en, retrieved on 4 September 2024.
9. European Commission (2022-c). *European Hydrogen Bank*, https://energy.ec.europa.eu/topics/energy-systems-integration/hydrogen/european-hydrogen-bank_en, retrieved on 5 September 2024.
10. Dash, S.K., Chakraborty, S., Elangovan, D. (2023). *A brief review of hydrogen production methods and their challenges*. *Energies*, 16(3), 1141.

11. Erdoğan, A., Güler, M.G. (2023). *Optimization and analysis of a hydrogen supply chain in terms of cost, CO_2 emissions, and risk: the case of Turkey*. In *International Journal of Hydrogen Energy*, 48(60), 22752-22765.
12. European Environment Agency (2023). *Green bonds*, https://www.eea.europa.eu/en/analysis/indicators/green-bonds-8th-eap?activeAccordion=546a7c35-9188-4d23-94ee-005d97c26f2b, retrieved on 18 September 2024.
13. European Hydrogen Observatory (2023). *The European Hydrogen Landscape*, https://observatory.clean-hydrogen.europa.eu/sites/default/files/2023-11/Report%2001%20-%20November%202023%20-%20The%20European%20hydrogen%20market%20landscape.pdf, retrieved on 17 September 2024.
14. France Hydrogène (2023). *National Hydrogen Strategy*, https://s3.production.france-hydrogene.org/uploads/sites/4/2023/10/France-Hydrogene_National-Hydrogen-Strategy_EN.pdf, retrieved on 19 September 2024.
15. H2 Energy News (2022). *15 French hydrogen projects selected from 100 European projects*, https://energynews.biz/15-french-hydrogen-projects-selected-from-100-european-projects/#:~:text=And%20among%20more%20than%20100%20projects%20submitted%20to,Flins-sur-Seine%20%28Hyvia%20%E2%80%93%20Renault%20Group%20and%20Plug%20Power%29, retrieved on 19 September 2024.
16. Hritsyshyna, M., Hutarevych, N. (2021). *Legal regulation of hydrogen in Germany and Ukraine as a precondition for energy partnership and energy transition. Energies*, 14(24), 8331.
17. Hydrogen Central (2024). *Launch of research project on green hydrogen production technologies the largest of its kind – Netherlands*, https://hydrogen-central.com/launch-of-research-project-on-green-hydrogen-production-technologies-the-largest-of-its-kind-netherlands/, retrieved on 19 September 2024.
18. Hydrogen Insight (2024-a). *Analysis | Which green hydrogen projects received state-aid approval from the EU in the recent €7bn IPCEI round?*, https://www.hydrogeninsight.com/production/analysis-which-green-hydrogen-projects-received-state-aid-approval-from-the-eu-in-the-recent-7bn-ipcei-round-/2-1-1600680, retrieved on 5 September 2024
19. Hydrogen Insight (2024-b). *EU gives green light to €1 bn Dutch green hydrogen subsidy scheme*, https://www.hydrogeninsight.com/policy/eu-gives-green-light-to-1bn-dutch-green-hydrogen-subsidy-scheme/2-1-1684243, retrieved on 5 September 2024
20. Hydrogen Insight (2024-c). *Germany grants €4.6 bn to 23 green hydrogen projects after EU approval*, https://www.hydrogeninsight.com/policy/germany-grants-4-6bn-to-23-green-hydrogen-projects-after-eu-approval/2-1-1677658, retrieved on 16 September 2024.
21. International Renewable Energy Agency/IRENA (2020). *Green Hydrogen – A guide to policy making*, https://www.irena.org/publications/2020/Nov/Green-hydrogen, retrieved on 10 September 2024.
22. Invest in Spain (2024). *Over 200 companies to promote 650 green hydrogen projects in Spain*, https://www.investinspain.org/content/icex-invest/en/noticias-main/2024/enagas.html, retrieved on 20 September 2024.

23. Jain, A.K. (2010). *Data clustering: 50 years beyond K-means*. *Pattern recognition letters*, 31(8), pp. 651-666.
24. Ji, M., Wang, J. (2021). *Review and comparison of various hydrogen production methods based on costs and life cycle impact assessment indicators*. In *International Journal of Hydrogen Energy*, 46(78), 38612-38635.
25. Madeira, S.C., Oliveira, A.L. (2004). *Biclustering algorithms for biological data analysis: a survey. IEEE/ACM transactions on computational biology and bioinformatics*, 1(1), pp. 24-45.
26. Münster, M., Bramstoft, R., Kountouris, I., Langer, L., Keles, D.&Schlautmann, R., ..., Rasmusson, H. (2024). *Perspectives on green hydrogen in Europe – during an energy crisis and towards future climate neutrality. Oxford Open Energy*, 3, oiae001, https://academic.oup.com/ooenergy/article/doi/10.1093/ooenergy/oiae001/7595745, retrieved on 20 September 2024.
27. Murtagh, F., Legendre, P. (2014). *Ward's hierarchical agglomerative clustering method: which algorithms implement Ward's criterion?* In *Journal of classification*, 31, pp. 274-295.
28. Pilavachi, P.A., Chatzipanagi, A.I., Spyropoulou, A.I. (2009). *Evaluation of hydrogen production methods using the analytic hierarchy process*. In *International Journal of hydrogen energy*, 34(13), 5294-5303.
29. Reda, B., Elzamar, A.A., Al Fazzani, S., Ezzat, S.M. (2024). *Green hydrogen as a source of renewable energy: a step towards sustainability, an overview*. *Environment, Development and Sustainability*, 1-21.
30. The Federal Government (2024). *National Hydrogen Strategy, Energy from climate-friendly gas*, https://www.bundesregierung.de/breg-en/service/hydrogen-technology-2204238, retrieved on 20 September 2024.
31. United Nations (2023). *Gothenburg Green Bonds|Sweden*, https://unfccc.int/climate-action/momentum-for-change/financing-for-climate-friendly/gothenburg-green-bonds, retrieved on 18 September 2024.
32. Vadaszi, M., Szunyog, I., Szombati-Galyas, A.B. (June 2023). *The Role of Hydrogen Connected to the Existing Natural Gas Infrastructure in the Hungarian Energy Transition*. In *2023 – 19th International Conference on the European Energy Market (EEM)* (pp. 1-5). IEEE.

DIGITAL LITERACY AND RESILIENCE AGAINST DISINFORMATION AMONG NATO MILITARY PERSONNEL

Colonel Associate Professor Petko DIMOV, PhD

Director of the Distance Learning, Language Training, and Qualification Department, Rakovski National Defence College, Sofia, Bulgaria

Colonel Associate Professor Georgi MARINOV, PhD

Department of Logistics, Rakovski National Defence College, Sofia, Bulgaria

DOI: 10.55535/RMT.2024.4.25

This article examines the digital literacy and resilience to disinformation among NATO military personnel, with a particular focus on the emerging challenges related to social media and search engine platforms. By analysing data collected in 2019 and comparing it to findings from a 2023 survey, the research identifies key trends in social media engagement, the capacity to recognize disinformation, and the strategies used to evaluate the credibility of online content. The results demonstrate that while a substantial proportion of military personnel actively use social media, there remains a significant deficiency in their ability to critically assess and verify the authenticity of the information they encounter. The study underscores the ongoing risks that disinformation poses to NATO's information security framework and stresses the urgent need for comprehensive digital literacy training programmes. The recommendations suggest implementing mandatory training to enhance critical thinking and analytical skills regarding information, alongside the development of specialized teams within NATO military structures dedicated to monitoring and combating disinformation.

Keywords: digital literacy; disinformation; military personnel; NATO; social media;

INTRODUCTION

The phenomenon of disinformation has increasingly become a focal point of academic research, particularly considering the rapid evolution of digital technologies and Artificial Intelligence. These advancements have substantially facilitated the creation and dissemination of false information, posing significant risks to information security and societal stability (Bradshaw, Howard, 2021). Military personnel, due to their pivotal societal roles, are often the targets of disinformation campaigns aimed at eroding morale and operational efficiency within military units (NATO Strategic Communications Centre of Excellence, 2022).

According to Martínez-Bravo et al. (2022), digital literacy encompasses a broad range of competencies that are crucial for successful functioning in the modern information society, including information literacy, technological literacy, cybersecurity, digital communication, content creation, critical thinking, digital financial literacy, and ethics and responsibility in the digital environment. (Martínez-Bravo et al., ib.)

Considering the already documented relationship between digital literacy and efforts to mitigate the effects of disinformation, this study aims to explore in greater depth the interconnection between digital skills, technological competence, and the ability of military personnel not only to recognize but also to critically evaluate and respond to disinformation. Specifically, the research emphasizes the hypothesis that service members with higher digital literacy and superior skills in Internet technologies are more capable of identifying disinformation in social media and search engines compared to those with lower digital literacy and weaker technological skills.

The benefits of this research extend beyond the military, contributing to a deeper understanding of the factors that influence resilience to disinformation and aiding in the development of more effective strategies to enhance this resilience. Such outcomes are valuable not only for the Armed Forces but also for society at large, as they contribute to greater security and stability within the digital environment.

This study employs a mixed-method approach, drawing on data from a 2019 NATO Command post exercise conducted in Poland. A survey comprising both closed and open-ended questions was administered to a sample of 5,844 respondents

– participants from various countries involved in the exercise[1]. The aim of this survey was to better understand the preferences, practices, and motivations of these participants in focusing on their duties rather than on unregulated news from the surrounding media environment. Military personnel represent a unique group of news consumers who can significantly impact national security during crises.

Building on this foundation, the present study focuses on how military personnel acquire, evaluate, and critically engage with news on social media and the role these activities play in their lives. It is crucial to investigate how these service members locate, verify, and ultimately trust news, as well as their ability to distinguish between *"fake news"* and *"real news".*

The research addresses the following three questions:

❖ *How do military personnel conceptualize what constitutes "news" and its implications?*

❖ *How do military personnel interact with and experience news on social media platforms?*

❖ *How do military personnel assess the credibility of online content?*

METHODOLOGY

The current research is based on data collected in 2019 during the largest International Logistics Command post exercise in NATO, *"Capable Logistician 19"*, in Poland (3-13 June 2019), as we have mentioned (NATO, 2019). These data were subsequently compared with a more recent survey conducted by the European Defence Agency (EDA) in 2023, covering 1,200 military personnel from 27 EU member states (EDA, 2023). The first sample includes responses from 360 military personnel from 23 countries who completed an anonymous online survey with English-language questions conducted by us. The survey contained 48 questions, and only 16 of them were used for the current research. 3,450 military personnel participated in this exercise, and to determine the size of the representative sample, the study authors used the non-returnable small population formula (Atanasov, Kaloyanov, 2020).

[1] The questionnaire is part of a larger research project. Because of the scope and confidentiality of the study, the authors cannot provide detailed information (A.N.).

$$n = \frac{Z^2 N * p(1-p)}{\Delta^2 N + Z^2 p(1-p)} = \frac{1{,}96^2 3450 * 0.25(1-0.25)}{\Delta 0{,}05^2 1100 + 1{,}96^2 0{,}25(1-0{,}25)} = 174{,}74, \quad (1)$$

where "z" is the guarantee multiplier corresponding to the chosen confidence level. In the general case, with a guaranteed probability of 95%, 1.96 is assumed (Gatev, 1995);

"p" is the relative proportion of units expected to have violations and is assumed to be 0.25;

"Δ" is the maximum stochastic error for the study assumed to be 0.05;

"N" – general population of all military personnel registered in the exercise, which are 3,450 people from 30 countries.

From the calculations, the 360 received responses to the questionnaires are significantly more than the required 174.74 to be a representative sample with a guaranteed probability of 95% and a confidence interval of 5%, which is quite sufficient for the needs of the present study.

In addition, the validity of the results is ensured by the fact that the survey was anonymous and military personnel from 23 countries out of 30 participated in it: Bulgaria, Bosnia and Herzegovina, Great Britain, Canada, Denmark, Czech Republic, Georgia, Hungary, Germany, Spain, Estonia, Finland, France, Italy, Lithuania, Latvia, Poland, Romania, Serbia, Slovakia, Sweden, Ukraine and Croatia. The second sample is significantly larger and serves to validate the obtained results.

RESULTS

To determine the level of social media usage among military personnel in 2019, respondents were asked whether they had accounts on any social media platforms and to specify which ones. Out of 360 military personnel, 306 (85%) confirmed having an account on a social network, while 54 (15%) did not. Among those with social media accounts, 220 (72%) used Facebook, 70 (23%) used Instagram, 8 (3%) used Snapchat, 7 (2%) used Twitter, 2 (1%) used VKontakte, 19 (6%) used Viber, 23 (7%) used WhatsApp, 8 (3%) used LinkedIn, and 3 (1%) used Messenger *(figure 1)*.

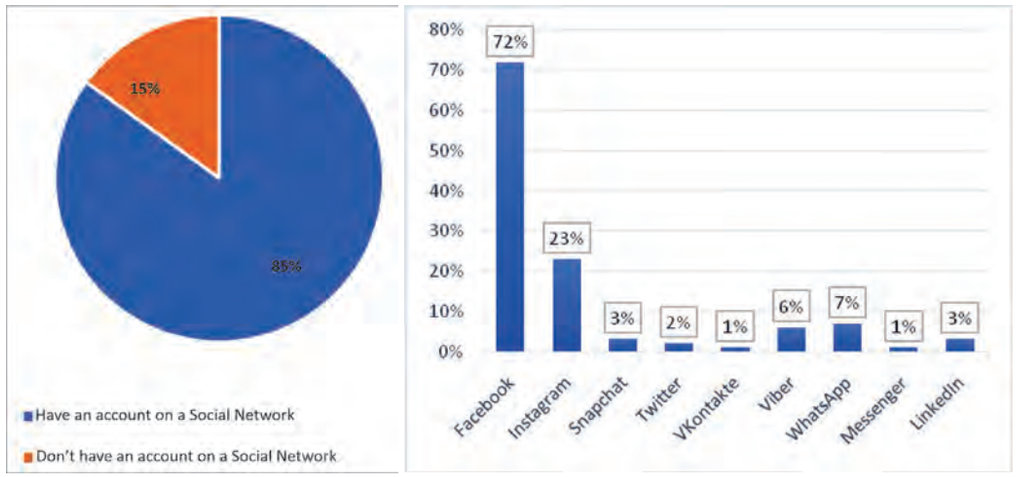


Figure 1: Distribution of military personnel with social media accounts: on the left, overall distribution; on the right, by type of social media (authors' design)

The EDA study from 2023 reported an increase in this percentage to 92%, with growing popularity of platforms such as TikTok (18%) and LinkedIn (15%) among military personnel (European Defence Agency, 2023). This indicates that social media is becoming a primary channel for receiving information or disinformation. While Facebook and Instagram remain the dominant platforms, a particularly concerning 1% of military personnel obtain information from the Russian social network VKontakte.

To assess the level of disinformation recognition, respondents were next asked whether they had ever encountered misleading or false information on social media. In 2019, 319 (89%) reported having encountered such information, while 41 (11%) said they had not or were unaware of it *(figure 2)*. It suggests that military personnel are aware of the risks of disinformation on social media. The 2023 data showed a slight increase to 93%, which may be attributed to heightened awareness or the growing amount of disinformation online (European Defence Agency, 2023).

To explore the frequency of information verification, respondents in the 2019 NATO Command post exercise in Poland were asked how often they verify the information they see on social media before sharing it. Only 54 (15%) of the military personnel confirmed that they verified information, while a significant 306 (85%) did not! *(figure 3).*

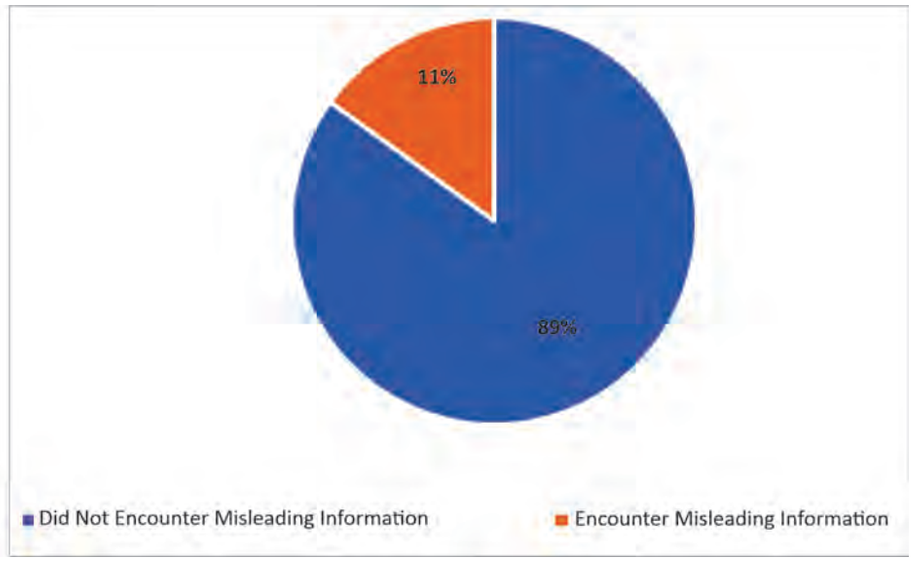


Figure 2: Percentage of those who have encountered disinformation online (authors' design)

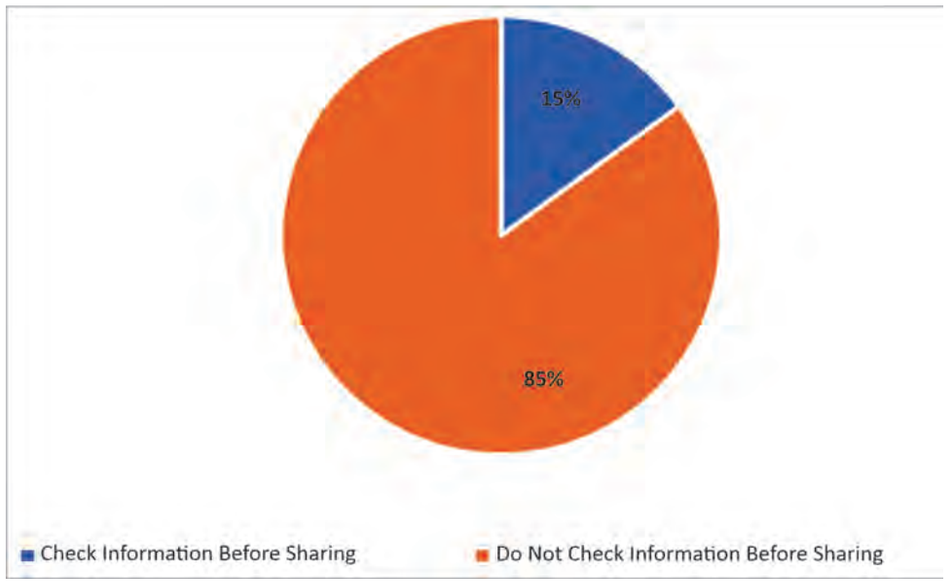


Figure 3: Percentage of military personnel who verify information before sharing it on social media (authors' design)

Despite being aware of the risks of disinformation and encountering it on social media, a very small percentage of military personnel verify the information they see before sharing it.

One of the most concerning aspects of the 2019 study is that only 15% of military personnel verify information before sharing it on social media. Data from 2023 shows some improvement, with 28% of respondents confirming that they regularly verify information before sharing it (European Defence Agency, 2023). However, this percentage remains unacceptably low given the importance of information security in the military context.

When asked which search engine they use most frequently, 334 (93%) of military personnel cited Google, 9 (2%) mentioned Qwant, and the rest were distributed among Seznam, Yahoo, Startpage, Safari, Yandex, and Netscape, each receiving less than 1%. This underscores Google as the main channel for receiving information or disinformation on the Internet. Search engines do not directly create disinformation, but their algorithms can inadvertently amplify it, as their ranking systems prioritize content based on engagement, popularity, and relevance, which can favour sensational or misleading information. Disinformation spreaders exploit search engine optimization (SEO) to rank higher in results. Additionally, search engines index vast amounts of unverified user-generated content, making it easy for false information to spread. Monetization strategies also encourage clickbait, which boosts disinformation further due to high traffic.

In a follow-up question on whether they had ever encountered misleading or false information in search engine results, 292 (81%) of military personnel confirmed they had, while 68 (19%) said they had not. These results are similar to those seen in social media interactions.

Respondents indicated that in Lithuania, false news predominantly concerns their history or historical figures, particularly partisans. Political leaders are the second most common target, especially in Eastern European countries. A persistent theme is the claim that NATO cannot protect them. In the United Kingdom, there are issues with influencers citing Russian propaganda sites such as Sputnik.ru. Americans primarily encounter disinformation related to Trump, while in Canada, respondents were generally unaware of false news.

When asked if they use cloud storage services such as Google Drive, iCloud, OneDrive, or others, 245 (68%) of military personnel confirmed they do, while 115 (32%) do not. Of those using cloud storage, 81 (33%) use iCloud most frequently,

93 (38%) use OneDrive, 180 (73%) use Google Drive, and 6 (2%) use Dropbox. These results suggest that digital literacy may influence the ability to recognize disinformation in social media and search engine results.

Google remains the dominant search engine, both in 2019 (93%) and in 2023 (89%), despite a slight decline in favour of privacy-focused alternatives (EDA, 2023). The use of cloud storage services increased from 68% in 2019 to 79% in 2023, with a greater variety of platforms being utilized.

Respondents were asked to determine how disinformation is detected, *"How do you assess the credibility of the information you share on your profiles?".* It was found that 73% verify the source of the news, 61% compare the news across multiple sources, 54% read the entire article before making a decision, 34% check the URL, 27% monitor comments, 23% consider the number of likes, and 41% conduct reverse image searches. The percentages exceeded 100% because respondents used multiple methods of verification. This indicates a certain level of digital literacy and knowledge of available tools *(table 1)*.

Table 1: How do you assess the credibility of the information you share on your profiles?
(authors' design)

Answers	Respondents %
I check who posted or tweeted the news	73
I read the whole news from beginning to end and then decide	54
I compare the news from several sources	61
I track the URL, date, or hashtag	34
I read the comments below the post	27
I observe how many times the news has been liked	23
I do a reverse Google search on the image used	41

The comparison between 2019 and 2023 data shows a positive trend in using more sophisticated methods to assess the credibility of information. For example, the percentage of military personnel conducting reverse image searches increased from 41% in 2019 to 58% in 2023 (Ib.).

DISCUSSION

The primary objective of this study was to examine the level of digital literacy among military personnel and whether it impacts their ability to recognize disinformation on social media and web search engines. The results indicate that the majority of military personnel have social media accounts, with Facebook being the most frequently used platform. Most respondents understand the risks of disinformation on these platforms; however, only a small percentage verify the information they see on social media before sharing it. This behaviour may indicate a lack of digital literacy.

The comparative analysis reveals both positive trends and ongoing challenges in the realm of digital literacy and resilience to disinformation among NATO military personnel. The increased use of social media and cloud services highlights the need for continuous updates to cybersecurity policies and digital literacy training.

Despite observed improvements in the methods used to assess the credibility of information, there remains a significant gap between recognizing disinformation and taking active steps to prevent its spread. This discrepancy underscores the need for more targeted educational programmes focused on critical thinking and media literacy in the digital age.

One of the key findings of the study is that Google is the most widely used search engine among military personnel. It aligns with other research showing Google as the most popular search engine globally (Stat Counter Global Stats). However, the majority of military personnel reported encountering misleading or false information in search engine results, indicating that additional security measures should be considered when presenting information on websites.

In line with the study's goal to investigate the relationship between digital skills and the ability of military personnel to critically evaluate and respond to disinformation, the use of cloud storage technology by military personnel, particularly Google Drive, plays a crucial role in enhancing operational efficiency and collaboration. However, while this reliance on digital tools reflects a positive development in terms of technological competence, it also introduces potential vulnerabilities. These cloud services, if not properly secured, may expose sensitive data to cyberattacks, which can be exploited as part of broader disinformation campaigns. Therefore, strengthening cybersecurity measures is essential to ensure that the use of such technologies does not undermine efforts to counter disinformation.

This study contributes to the field by demonstrating the relationship between digital literacy and the ability to recognize disinformation among military personnel. The findings can be used to develop effective digital literacy training programmes for military personnel, as well as to inform security policies that reduce the risk of disinformation when using social media, search engines, and cloud storage technologies. Moreover, future research should consider other factors that may influence the ability to recognize disinformation, such as educational background and professional experience.

RECOMMENDATIONS

The key conclusions of this study are that the majority of military personnel have social media accounts and frequently use them, yet only a small percentage verify the information they see before sharing it, despite being aware of the risk of disinformation. It suggests that digital literacy among military personnel is insufficient, and measures need to be taken to improve it.

On the other hand, most military personnel have encountered misleading or false information on social media and in search engine results, indicating that disinformation is widespread and poses a serious threat to NATO's Information Security in conducting Command post exercises.

A comparison with more recent studies confirms that disinformation continues to be a significant threat to the information security of NATO military structures. Despite observed improvements in some aspects of digital literacy, there are still significant gaps that need to be addressed.

This aspect underscores the need for a comprehensive digital literacy training programme tailored for military personnel, aimed at enhancing their ability to recognize and combat disinformation. Some countries, such as Lithuania, Latvia, and Estonia, have developed programmes in this area, though not to their full extent. Special attention should be given to improving their skills in navigating and critically evaluating content on social media platforms and in search engine results. This programme should be mandatory for all military personnel and conducted before major exercises to ensure that the staff is aware of the latest trends and disinformation techniques. The programme should not only cover technical skills but also foster critical thinking and the ability to analyse information in the digital environment.

Another recommendation is to promote the use of reliable information sources and provide military personnel with access to such sources. It will allow them to receive accurate and up-to-date information, enabling them to make more informed decisions.

Additionally, it is recommended that specialized teams within the military structures should be established to monitor and counter disinformation and enhance cooperation among NATO member states in the field of information security.

In conclusion, disinformation remains a serious threat to security, and digital literacy is essential to prevent its spread. The study shows that the majority of military personnel lack sufficient digital literacy, and measures need to be taken to improve it. The recommendations proposed in this study will help the Armed Forces address disinformation and ensure allied security.

CONCLUSIONS

The most important finding of this study is that military personnel's news consumption is both multimodal and multi-social; they receive news from their colleagues just as much as from social media platforms.

While most military personnel recognize that a free press is essential to democracy and contributes to the resilience of the European Union and NATO, deep political polarization makes them suspicious of certain news sources. A significant number of them even question the spread of *"fast news"* and the fragmented coverage often found on social media platforms.

These aspects underscore the complexity of their media environment and the need for enhanced digital literacy to navigate it effectively.

BIBLIOGRAPHICAL REFERENCES:

1. Atanasov, A., Kaloyanov, T. (2020). *Metodologichnipodhodinaizvadkoviteizsledv ania za izvarshvanenaproverkinabenefitsientitena* (Metodologiq hniподходина извадковите изследван*ия за извършване напроверкинабенефициентитена).* OP RChR 2014-2020. Nauchnitrudovena UNSS, 42-58. Sofia: UNSS, http://unwe-research-papers.org/uploads/ResearchPapers/02_Atanas%20Atanasov,%20Todor%20Kaloyanov.pdf [in Bulgarian], retrieved on 27 July 2024.
2. Bradshaw, S., Howard, P.N. (2021). *The Global Disinformation Order: 2021 Global Inventory of Organised Social Media Manipulation*. Oxford: Oxford Internet Institute.
3. European Defence Agency/EDA (2023). *Digital Literacy and Disinformation Resilience Among Military Personnel in EU Member States*. Brussels, retrieved on 27 July 2024.

4. Gatev, K. (1995). *Vavedenie v statistikata*. Sofia, Lia.
5. NATO. (2019). *NATO Exercise Cyber Coalition 2019*. Brussels: NATO, https://www.nato.int/cps/en/natohq/news_166827.htm?selectedLocale=en, retrieved on 27 July 2024.
6. NATO Strategic Communications Centre of Excellence. (2022). *Countering Information Influence Activities: A handbook for communicators*. Riga: NATO StratCom COE.
7. *Search engine market share worldwide.* Stat Counter Global Stats. (n.d.), https://gs.statcounter.com/search-engine-market-share, retrieved on 17 October 2024.

THE NORDIC RESISTANCE MOVEMENT AS A THREAT TO EUROPEAN AND INTERNATIONAL SECURITY

Iulian DINULESCU, PhD
"Mihai Viteazul" National Intelligence Academy, Bucharest
DOI: 10.55535/RMT.2024.4.26

The Nordic Resistance Movement (NRM) is a Scandinavian neo-Nazi organization that promotes a violent, National Socialist ideology, supported by a hijacking of Nordic religious symbolism. The article examines how the NRM reinterprets pre-Christian mythology and symbols, such as runes and Viking myths, to legitimize ideas of racial superiority and motivate its followers to take violent action. The NRM not only distorts Nordic spirituality, but uses this symbolism to construct an exclusive racial identity and a form of heroic "sacrifice" that justifies violence against ethnic minorities and political opponents. In addition, the article highlights the transnational impact of the NRM, noting its links to other extremist groups and its designation as a terrorist organization by the United States Department of State. This designation reflects global concerns about right-wing extremism and the associated security risks. The misuse of religious symbols amplifies the risk of radicalization and violence among disillusioned youth, drawing them towards violent ethnic nationalism. The article also offers an analysis of international efforts to counter violent extremism and the need for expanded cooperation to combat this threat.

Keywords: terrorism; extreme right; Nordic Resistance Movement; ideology; violence; religion;

METHODOLOGICAL CONSIDERATIONS

Theoretical foundation. The study draws on several relevant theoretical frameworks from the field of security and extremism studies with the aim of better understanding how the Nordic Resistance Movement (NRM) uses religious and mythological symbolism to justify and propagate extreme violence. A relevant theoretical approach is the Securitization Theory (Buzan, Waever, de Wilde, 1998, pp. 21-47), which analyses the process by which a state transforms certain situations into security issues through official discourse and actions. In the case of the NRM organization, securitization can be interpreted as an analytical framework for understanding how authorities in the Nordic states, the USA, and other countries view the group as a threat to national security. Thus, the authorities' use of the concept of securitization reflects concerns about the ideology and international activities of NRM, with potential implications for transnational stability and security.

Also, Radicalization Theory (McCauley, Moskalenko, 2008, pp. 415-433) provides a solid theoretical framework for understanding the psychological and social processes by which disillusioned youth are drawn to extremist ideologies. The NRM uses a combination of mythology and symbolic violence to build a strong collective identity, giving young people a sense of belonging and purpose. This is a form of identity mobilization, specific to radical groups, which exploits the fear of cultural and social changes to justify violent acts. In addition, the Theory of Asymmetric Conflict (Kaldor, 2006, pp. 1-18) can be discussed, which explains how smaller and poorly organized groups, such as the NRM, resort to violent and terrorist strategies to undermine democratic institutions. These theoretical frameworks are essential to understanding how the NRM not only distorts religious symbols, but also instrumentalizes these symbols to create a global security threat. In the context of security theories, the right-wing extremism of the NRM is not just an isolated phenomenon, but one that causes political and social instability at the international level.

The theoretical and methodological background section clarifies that this paper analyses the Nordic Resistance Movement as a threat to European and international security. The central research question is to investigate how the NRM instrumentalises Nordic symbolism to legitimize a violent ideology with the aim of influencing and destabilizing social and political structures. For this

purpose, the paper coherently applies three theoretical frameworks. Securitization theory explains how certain states view NRM as a security threat by analysing the discourses through which the organization is publicly presented as a risk to social order. Radicalization theory helps to identify the psychological and social processes by which the NRM attracts supporters, using Nordic symbols to confer a sense of belonging. Finally, the theory of asymmetric conflict underpins the analysis of the strategies through which the NRM causes instability and promotes its extremist agenda, undermining democratic institutions. This integrated theoretical framework facilitates deep and grounded analysis, providing coherent and structured answers to the stated research questions.

Methodology. This article uses a qualitative research methodology based on documentary analysis and case study to investigate the actions and ideology of the Nordic Resistance Movement. The research draws on extensive secondary sources, including security reports, academic studies, media documents and field reports produced by international organizations that monitor the activity of extremist groups. A central element of the methodology is discourse analysis, whereby official NRM publications, websites and online propaganda materials are examined to understand how religious and mythological symbolism is used as a tool for recruitment and mobilization. An important aspect of the method is the case study of extremist violence committed by NRM members. The article examines several major violent incidents, such as the 2016 and 2017 Gothenburg bombings, which involved members of the NRM. By investigating these cases, it aims to demonstrate the direct link between the extremist ideology promoted by the NRM and the violent actions they inspired. It allows not only to understand how extremist discourse is transformed into concrete actions, but also to identify patterns of radicalization among group members. In terms of source selection, the research is based on reports produced by recognized organizations such as the Counter Extremism Project and ADL, which provide a detailed assessment of NRM activities and its transnational impact. Another important methodological element is comparative analysis. The NRM is analysed in relation to other similar extremist movements in Europe and the United States of America, such as the Russian Imperial Movement and Der Dritte Weg. It provides the context and allows the identification of common strategies used by these groups, such as the use of online propaganda and religious symbols to mobilize and radicalize new members.

Limitations of the research. Although this analysis provides a detailed picture of NRM activities and ideology, there are some limitations. One of them is restricted access to the group's internal primary sources, such as their internal communications

and organizational strategies, which are difficult to obtain due to the clandestine nature of the organization. Also, the article is largely based on secondary sources, which may bring the risk of subjectivity on the part of the authors of these reports. However, by triangulating sources and selecting internationally recognized studies and reports, these limitations are minimized.

THE NORDIC RESISTANCE MOVEMENT – A THREAT TO EUROPEAN AND INTERNATIONAL SECURITY

The Nordic Resistance Movement (NRM) represents an alarming phenomenon in the landscape of contemporary extremism, with deep roots in nationalist and neo-Nazi ideologies. Although founded in Scandinavia, this far-right organization has transformed over the course of more than two decades into a well-organized transnational network known for its radical rhetoric and violent actions. Through a combination of propaganda, paramilitary recruitment and direct attacks, the NRM poses a serious threat to national and international security, being involved in a constant effort to destabilize democracy in the Nordic countries.

The NRM is a far-right organization with deep roots in the racial nationalism and far-right traditions of Scandinavia. Kacper Rekawek and Morgan Finnsiö say the NRM is a revolutionary neo-Nazi group that aims to overthrow democracy in the Nordic countries and replace it with a Nazi dictatorship. Despite their claims of preference for legal methods, they are prepared to resort to violence to achieve their goals. The group reveres historical figures such as Adolf Hitler and Corneliu Zelea Codreanu and, with minor modernizations, remains a classic exponent of eo-Nazi ideology (Rekawek, Finnsiö, 2024). The NRM poses a significant security risk due to its extremist ideology, violent actions and paramilitary structure. The group promotes deeply anti-Semitic and anti-immigrant rhetoric, attempting to spread these ideas through propaganda and violent actions, including bombings and physical attacks (Counter Extremism Project, 2024). Over a quarter of a century, the NRM has evolved into a complex transnational organization with a strict hierarchical structure and paramilitary elements. The group has been responsible for violent attacks against citizens, minorities, and democratic institutions, posing a major threat to public security (ADL, 2022). Founded in 1997, the NRM has survived various difficulties and divisions that could have destroyed other similar groups. The group has a rigid and hierarchical structure, being known for its violence in both rhetoric and practice. It has carried out brutal attacks in the Nordic countries, including lethal actions (Rekawek, Finnsiö, ib.). The NRM uses propaganda effectively and presents itself as a bold and feared organization, taking advantage of the relatively

lax Swedish context regarding right-wing extremism. It allows them to capture the attention of extremist observers and inspire other like-minded groups (Ib.). After a peak in 2018, the NRM suffered from internal divisions and recruitment problems, but stabilized in 2024, under a new leader, Fredrik Vejdeland. Although smaller compared to the peak period, they remain an active and violent threat (Ib.).

On 14 June 2024, the US Department of State designated the NRM and three of its leaders as Specially Designated Global Terrorists. The action highlights racially or ethnically motivated violent extremist threats and the transnational impact of violent white supremacy. The decision is the result of in-depth consultations with the US's European partners and is intended to intensify international measures against these threats (Miller, 2024). Designation as a terrorist group will affect the NRM's financial interactions and increase international monitoring. This designation will complicate the group's activities and consume their resources (Rekawek, Finnsiö, ib.). It marks the first time the Biden administration has labelled a far-right organization in this way. Previously, the only far-right organization so designated was the Russian Imperial Movement (RIM), in April 2020, during the Trump administration (Blazakis, 2024-a). The NRM designation was made against a backdrop of increased right-wing extremism violence in Europe, including recent attacks and the rise in political influence of far-right groups. This action reflects a more proactive approach by the Biden administration in combating international threats (Blazakis, 2024-b). The NRM maintains links with various extremist groups in Sweden, but also in other European states, such as Der Dritte Weg, and they have participated in extremist events in several European countries. In the past, they had relations with the Russian Imperial Movement, but these contacts became more discreet after the designation of the Russian Imperial Movement as a terrorist group (Rekawek, Finnsiö, ib.). NRM and RIM had close connections, including collaborations in paramilitary training and attending conferences with anti-Semitic content. These links point to a complex international network of right-wing extremism that shares resources and ideologies (Blazakis, 2024-a).

Despite domestic challenges and international pressure, the NRM remains a strong exponent of violent far-right extremism. With its designation as a terrorist group in 2024, the United States of America signals an intensification of global efforts to combat white supremacy and extremist groups. However, its paramilitary structure, transnational ties, and commitment to violence continue to make the NRM a dangerous force capable of influencing and destabilizing security both locally and globally.

The Manipulation of Nordic Religious Symbols in the NMR's National Socialist Ideology: A Distorted View of Spirituality and Race

A central aspect of the movement is religious and mythological symbolism, which is used to reinforce ethnic identity and racial ideology. NMR uses pagan myths and symbols, especially from Norse mythology, such as the Tiwaz/Tyr and Yngvi/Ing runes, which reflect Norse gods and warrior dynasties (Kenes, 2020, p. 12). The NMR uses the *"Viking image"* to differentiate itself from European far-right ideologies that defend *"Christian civilization"*, replacing this tradition with a view focused on Norse mythology and culture (Ib.). The NRM articulates its ideology as a form of *"racial revolution"*, which is not only limited to political and social aspects, but also includes a religious component, promoting an anti-religious vision based on the rejection of traditional values and religious diversity (ADL, 2022). The main symbol of the NRM is the Tiwaz rune, which has links to Nazi-era religious symbolism, also used in the context of far-right ideology. It highlights the fact that National Socialist ideologies are often linked to perverted religious concepts (Ib.). The NRM considers traditional religion to be a tool of the *"global Zionist elite"* and part of structures it considers corrupt and hostile to the Nordic race. NRM ideology rejects traditional religious values and views them as part of the global problem they challenge, namely Jewish control of humanity (Ib.).

One of the founders of the NMR who led the organization between 1997 and 2015, Klas Lund, was also the editor-in-chief of *Folktribunen*, a magazine that between 1997 and 2002 was used by the Swedish Resistance Movement – the predecessor of the NRM, as a communication platform to disseminate the positions and the activities of the organization (Kenes, 2020, p. 7). Folktribunen promoted Corneliu Zelea Codreanu, the one who founded and led the Iron Guard, an ultra-nationalist and strongly anti-Semitic movement, founded in 1927 in Romania. Initially, this *"terrorist"* organization was called the Archangel Michael Legion, and its leader, Corneliu Zelea Codreanu, *"a Christian fanatic"*, wanted the formation of a state controlled by *"an elite"*, similar to *"a religious sect"* (Kenes, p. 8). Its ideology entailed the formation of a *"new man"*, and the Iron Guard was to play a central role in this revolution. Under his leadership, the organization was involved in numerous political assassinations and violent attacks, especially against Jews (Ib.). After carrying out a scientific research, Iulian Dinulescu concluded that neo-legionary religious fanaticism, based on the ideology of the Iron Guard, continues to be relevant through the combination of religious and ultra-nationalist ideas, the rejection of foreigners and anti-Semitism, and the promotion of a state based on white and Christian identity (Dinulescu, 2020, pp. 173-177).

The Vikings are presented as a central symbol in *"Nordic National Socialism"*, representing the *"Nordic race"*, ideals of masculinity and a cohesive male community, reinterpreted in a Nordic context. The Vikings are used to make Nazi ideology more acceptable in the Nordic context, removing exclusive associations with Germany and orienting it towards a Nordic cultural-historical identity (Kenes, p. 12). *"The religion of the Norse and Germanic gods"*, such as Odinism, *"is popular among skinheads because of its violent and warlike ethos"*, says Pollard (2016, p. 409). It is presented as *"a religion of warriors"*, in contrast to Christianity, considered *"a religion of slaves"* in *"Nietzschean terms"* (Ib.). The NMR rejects Christianity as a *"contagious mental disease"* and a *"form of spiritual AIDS"* that has weakened society's natural defences against external influences. Christianity is seen as a threat *"that must be fought by all means"* (Riis-Knudsen, 2010, p. 13; Lodenius, 2020, p. 152).

NRM focuses on reinterpreting old Nordic religious symbols to construct a *völkisch* identity, a concept that combines ethnicity with nationalism and mythology (Butters, 2023, pp. 60-61). This movement uses symbols from pre-Christian religions, especially Norse mythology and Norse paganism, in a process of re-signification that attempts to connect the idea of racial purity with the ancient beliefs of the Vikings (Ib., pp. 61-62). In this context, religious symbols are not only visual signs, but vehicles for transmitting an identity and spiritual message, being associated with esoteric beliefs that resonate with the idea of the superiority of the white race (Ib.). For example, the Norse runes, especially the Týr rune, are re-signified to symbolize courage, sacrifice and fighting for a cause deemed *"just"* by the movement. These symbols serve to construct a group religiosity, where spirituality is linked to ethnicity and belonging to a so-called pure Nordic race. The use of these symbols deepens the separation from the Christian religion, often criticized by NRM members, who prefer values related to Norse mythology and a glorified past, supposedly noble and unaltered by external influences (Ib., pp. 65-67).

This movement succeeded in using nationalist and national socialist ideology to define a *"religion"* of race and blood, linking spirituality to ethnic purity and racist ideas (Ravndal, 2019, pp. 21-22). The NRM is not a religious movement in the traditional sense, but embraces a National Socialist ideology centred on the creation of a white Nordic state. In the NRM view, religion is subordinated to extreme nationalism, and spiritual elements are marginalized in favour of the struggle for racial purity and the war against the perceived enemies of the white race (Bjørgo, Ravndal, 2020, p. 37). However, NRM members do not completely reject spirituality; they sometimes adopt a rhetoric related to Nordic identity, loosely connected to Nordic mythology and pagan traditions, but without an explicit religiosity.

Instead, the focus is on the idea of struggle and sacrifice for the *"survival of the Nordic race"* (Ib., pp. 39-40). The NRM is described as a radical nationalist movement that is not explicitly based on a formal religion, but on a belief system that invalidates human equality and promotes violence to protect an ethnically homogeneous state (Ranstorp, Ahlin, 2020, pp. 2-3). Although there is no formal religion associated with the movement, there is a rhetoric of *"sacrifice"* for the racial cause, which can be seen as a form of distorted spirituality used to legitimize violence against other ethnic and cultural groups (Ib., pp. 3-4). Religion plays an important role in NRM through the use of symbols associated with Norse mythology and Germanic paganism. These symbols, considered sacred by some, are used by others to promote a nationalist and supremacist vision. Some pagan communities, known as *"Heathenry"*, view these symbols as part of their spiritual identity, while other extremist groups use them to spread messages of racial hatred (Nikitins, 2020, p. 1). The spiritual ideology of the NRM is rooted in ancient Nordic mythologies, used not to express genuine religiosity, but to justify a false historical past based on racial purity (Ib., p. 6). This falsification of history includes the distortion of the relations between the Scandinavian peoples and the other ethnic groups, highlighting a racist ideology that denies the historical diversity and multiculturalism of ancient Scandinavia (Ib., p. 7).

Symbols such as the runes Týr, Sig and Odal are extremely important in the discourse and aesthetics of the NRM, having a dual function: on the one hand, they are used as identity symbols of the movement and, on the other hand, as means of legitimizing claims about racial superiority (Butters, pp. 65-66). For example, the Týr rune, which symbolizes war and victory, is used as the official emblem of the NRM, becoming a substitute for Nazi symbols, such as the swastika, which are banned in many countries (Ib.). Other symbols, such as the Odal rune, which symbolizes *"blood and soil"* (Blut und Boden), are directly associated with Nazi ideologies, being recontextualized to promote a nationalist and racist ideology based on racial purity and the ancestral connection to the land (Ib., pp. 66-67). Likewise, the Valknut, an ancient Viking symbol associated with heroic death and the afterlife in Norse mythology, was re-signified by NRM members to represent sacrifice and struggle for the white race, becoming a symbol of racial identity (Ib., pp. 67-68).

This appropriation of religious symbols from the Nordic past is a strategy by which the movement constructs an ideology that promotes a violent ethnic nationalism disguised as pre-Christian spirituality and religiosity (Ib., pp. 70-71). The use of runes and other symbols from Norse mythology, such as Valknut or Yggdrasil, is common in their public activities. These symbols are reinterpreted

and used to strengthen the link between the National Socialist ideology and the cultural and spiritual heritage of the Nordics (Ravndal, 2019, pp. 22-23). Nordic religious symbols are presented as a central element of their struggle to create a racially pure state, where ancient mythology becomes a source of legitimation for the movement's political goals (Ravndal, p. 25). Religious symbolism within the NRM is related to nationalist symbols and National Socialist ideology rather than a formal religion. The movement uses various cultural and historical elements from the Nordic past to legitimize its struggle. For example, symbols and rhetoric about *"race war"* are used as means of propaganda and recruitment (Bjørgo, Ravndal, 2020, pp. 39-40). This instrumentalization of historical symbols to support nationalist ideology shows how the NRM reinterprets cultural elements to promote extremism.

Although not based on traditional religious symbols, the movement uses a number of images and ideas that evoke Nordic identity and the struggle for the survival of the Nordic race. They include ideas about defending the *"sacred"* territory of the Nordic people, which must be protected against external influences (Ranstorp, Ahlin, 2020, pp. 4-5). Religious symbols, especially those from Nordic mythology, have been appropriated by supremacist groups, including the NRM. Among the symbols used are runes such as *"othala"*, which symbolizes ancestral heritage, and *"sowilo"*, associated with victory and honour (Nikitins, 2020, pp. 6-7). In the context of the NRM, these symbols are reinterpreted to promote the idea of racial purity and the creation of an ethno-nationalist state (Nikitins, p. 14). Religious symbols are diverted from their original meaning, becoming political instruments of extremism (Ib., p. 13). For example, *"Black Sun"*, a Germanic symbol, is frequently used by the NRM for fascist propaganda purposes (Ib., p. 5).

The NRM uses symbols associated with Nazi Germany, such as the swastika, in its public demonstrations and propaganda activities. Although the group does not operate primarily on a religious basis, their ideology of racial superiority and anti-Semitic rhetoric is presented in an almost religious manner, treating their mission to defend the *"Nordic people"* as a sacred goal. The NRM aims to preserve the purity of the Nordic race by using a distorted mythology of the Nordics, similar to the beliefs espoused by Nazi Germany (Counter Extremism Project, 2024). These symbols were revived to support their vision of a united and pure *"ethnically Nordic nation"*, reinforcing the idea of racial superiority. This form of religious symbolism is used as part of their ideological image, being an essential element in mobilizing supporters (The Guardian, 2024).

Thus, Nordic religious symbols such as the Týr and Odal runes are centralized by the NRM to legitimize its extremist ideology. These mythological symbols are reinterpreted to support ideas of racial superiority and ethnic nationalism, thus turning Norse mythology into a political tool of National Socialist extremism. The NRM is a neo-fascist and accelerationist organization that promotes violent ideologies and incitement to hatred, including through attacks on the rights of religious minorities. Although its primary activity is not religious in nature, the organization uses religious symbols and rhetoric to reinforce its extremist messages and influence.

The Ideology of Violence Promoted by the Nordic Resistance Movement

The NRM uses religious and mythological symbolism not only to legitimize its vision of the superiority of the white race, but also to distance itself from other European extremist movements through its Nordic and Viking specificity (Butters, pp. 71-72). By rejecting modern values and promoting a mythologized image of the Vikings as pure white warriors, the NRM promotes a form of extremism that finds its legitimacy in the idealized historical past of the Norse. It is also important to note that their ideology is not limited to the cultural level, but also includes direct calls for violent action against those considered enemies of the Nordic race (Ib., pp. 72-73). The NRM uses symbols such as the Týr rune or other Nordic runes to legitimize violence, seeing it as a form of sacrifice necessary to defend racial purity and Nordic identity (Ib., pp. 73-74). This is a recontextualization of racist ideologies from the Nazi era, where symbols were used to construct a mythology of racial superiority and the right to violence against those deemed inferior (Ib., pp. 74-75). The NRM is defined as a *"militant National Socialist"* movement, engaged in the *"extra-parliamentary struggle"* for a national revolution (Ravndal, p. 11). NRM actions include both legal activities, such as distributing leaflets and organizing marches, as well as violent acts against their political or the Nordic race enemies (Ib., pp. 26-27). Their strategy is based on the idea that they will be able to trigger radical change through violence and direct action when the time is right (Ib., p. 24). The NRM has no moral restrictions on the use of political violence, including mass murder, but refrains from acts of terrorism for strategic reasons (Bjørgo, Ravndal, 2020, p. 40). Its members are trained in street fighting and weapon handling, and some of the activists have committed acts of extreme violence, including fatal attacks (Ib., pp. 39-40).

The NRM actively promotes its National Socialist ideology through violent means. Despite claims that the movement does not engage in acts of terrorism, its members have been involved in several violent attacks on minorities and political

opponents. The NRM promotes a rhetoric of cultural and racial war, justifying the use of violence as a means of defending the Nordic race and destabilizing the existing political order (Ranstorp, Ahlin, pp. 5-6). The movement presents itself as a revolutionary alternative to parliamentary democracy, which it considers corrupt and inadequate to protect the interests of the Nordic people (Ib., pp. 6-7). The NRM uses religion as a vehicle to legitimize its extremist ideology. It is based on the myth of racial purity, a falsification of history that ignores interactions between Scandinavian peoples and other cultures (Nikitins, p. 7). This movement uses religious symbolism to promote a form of exclusivist religion, where Nordic deities and myths are reinterpreted to support the idea of racial superiority and war against the *"other"*, seen as a threat (Ib., p. 14). The group has a violent history, being involved in attacks on immigrants and political opponents. Among the most notorious attacks are bombings and physical assaults. The NRM promotes the violent overthrow of democracy and the establishment of a totalitarian regime inspired by the Third Reich. The group prepares militarily, organizes training camps and collects weapons, thus increasing the level of risk it represents. Their connections with other extremist groups in Russia increase their ability to carry out transnational violent actions (Counter Extremism Project, 2024). Examples of violent extremism in the group's past include major incidents such as the death of a 28-year-old man in Helsinki, Finland, after being attacked by members of the NRM, and a series of bombings in Gothenburg, Sweden, in 2016 and 2017, in which several members were convicted. This spate of violence demonstrates that the group's ideology directly manifests itself in terrorist actions, not just rhetoric (The Guardian, ib.).

The movement's involvement in acts of violence, including explosive attacks and direct confrontations with the police, led to increased tensions in society (Ravndal, pp. 27-28). Also, the NRM's links with other extremist groups outside of Scandinavia amplify the risks, turning them into a transnational organization (Ib., p. 15). This ability to organize and act transnationally increases security risks, especially in the context where NRM militants are willing to use violence to achieve their goals (Ib., p. 28). Although the movement avoids the use of terrorism for the time being in order not to be banned in all Scandinavian countries, it does not rule out its use in the future, depending on the evolution of the political situation. The NRM constantly tests its legal boundaries and is frequently involved in violent confrontations, especially in Sweden and Finland, where activists have been involved in attacks on minorities and political opponents (Bjørgo, Ravndal, pp. 40-41). The NRM also uses intimidation tactics such as subtle threats against politicians and journalists,

leading to undermining democracy and public safety (Ib., pp. 41-42). Although the organization suffered a decline in activity after the electoral failure of 2018, its members continue to be involved in violent actions and maintain links with other extremist groups in Europe and the United States of America (Ranstorp, Ahlin, p. 8). The use of religious symbolism for violent purposes is a strategy that makes the ideology of the movement attractive to a wide audience, especially young people disillusioned and attracted to the idea of a heroic and glorious past. This rhetoric not only supports acts of violence, but also glorifies them, legitimizing them through a distorted interpretation of Nordic spirituality (Butters, pp. 73-74).

The NRM is vehemently anti-Israel and pro-Hamas, holding Israel responsible for many of the global problems and admiring Hamas for its anti-Jewish and nationalist stances (Rekawek, Finnsiö, 2024). The NRM expresses some admiration for Hamas, not from a pro-Palestinian position, but from an anti-Semitic and nationalist perspective. Although Hamas is an Islamist group, the NRM values it because it is considered an anti-Jewish and anti-Israeli resistance group, according to their neo-Nazi ideology (Ib.). NRM is not just limited to hatred of Jews, but also hatred of Muslims and Arabs. Although the NRM presents itself as a white supremacist and nationalist group, their ideology is closely tied to religious and ethnic prejudice, including promoting conspiracy theories about negative Jewish influence on the world (Ib.). The group promotes a radical Nazi ideology, focusing on anti-Semitism, biological racism and eco-fascism. In its view, the NRM sees the *"Nordic race"* as threatened by a global Jewish conspiracy and views democracy and liberalism as destructive inventions created by Jews (ADL, 2022).

Therefore, this extremist ideology justifies its violent actions, seeing violence as a necessity to protect the Nordic race and destabilize the current political order. The NRM carries out violent activities against minorities and political opponents, promoting the rhetoric of a *"cultural war"* to restore a society based on National Socialism.

The Structure and International Ramifications of the Nordic Resistance Movement

The organization is structured into regional divisions, known as *"Nests"*, and has a centralized leadership with a supreme leader and regional councils. Despite periods of decline and internal strife, including a leadership coup in 2019 that led to the formation of a separate group, Nordic Strength, the NRM continues to be active and influential in the far-right movement (ADL, 2022). Its recent strategy has focused on expansion and public visibility, but electoral setbacks and internal conflicts have affected the organization's effectiveness. Anti-Semitism is a central element of NRM

propaganda, and the group uses multiple channels to spread its extremist messages (ADL, 2022). As the largest organization of its kind in this area, the NRM stands out for its transnational presence and extensive internet reach, which facilitates the recruitment of new members, their radicalization and *"incitement to violence"*. The organization has managed to maintain a core of around 200 active members in Sweden, Denmark and Norway. It also has significant supporters in Iceland and Finland. However, in Finland, the NRM was banned in 2020 due to violations of laws *"protecting human rights"* and *"minorities"*, against which the organization *"incited violence"* (Center on Terrorism, Extremism, and Counterterrorism, 2022).

The NRM represents a significant risk to people's security, being involved in violent and terrorist activities. In Finland, the movement was banned following acts of violence and attacks on immigrants and other minority groups (Butters, pp. 70-72). However, even in the face of legal bans, members continue to operate under other names or use alternative symbols to avoid legal repercussions, which demonstrates the fluidity of extremism and the difficulty of combating it effectively (Ib., pp. 72-73). The leader of NRM is Fredrik Vejdeland, who operates from Sweden, with subordinate leaders in the various divisions in other Nordic countries. Members of the organization have been arrested over time for their involvement in acts of violence, which contributes to the general perception of the NRM as a highly dangerous organization globally (Center on Terrorism, Extremism, and Counterterrorism, 2022).

The NRM also uses social media to spread hate messages and mobilize new followers, which amplifies the risk of radicalization and violence in Swedish society. The Swedish authorities believe that the threat of right-wing extremism has increased in recent years, and the NRM remains a central actor in this extremist milieu (Ranstor, Ahlin, pp. 9-10). The use of religious symbols as tools of recruitment and radicalization makes the NRM perceived not only as a nationalist terrorist group, but also as a global threat (Nikitins, p. 15). The presence of these symbols at far-right events such as *"Unite the Right"* in Charlottesville demonstrates how sacred symbols can be hijacked to promote violence and social conflict (Ib., pp. 6-7).

Religion, especially paganism, is under pressure due to association with extremist movements such as the NRM. Pagan practitioners who reject hateful ideologies feel alienated and fight to protect their sacred symbols from misappropriation. For example, groups such as *"Heathens United Against Racism"* and *"The Alliance for Inclusive Heathenry"* began to organize protests against the infiltration of extremist ideologies into their religion (Nikitins, p. 3). At the same time, religious organizations in Sweden and Iceland have publicly stated that they do not want

their religion to be associated with racism or militarism (Ib., p. 14). Many of the religious symbols used by the NRM have become, because of their association with extremism, difficult to reclaim by pagan religious communities. For example, *"othala"* is considered one of the most contaminated runes, being frequently used in a supremacist context (Ib., pp. 6-7).

NRM is a direct security threat not only in Scandinavia, but also in the rest of Europe. The group recruits its followers, especially through online platforms, trying to radicalize vulnerable people. The spread of their extremist ideology creates a generalized threat at European level, as the group also inspires other far-right organizations, amplifying the risk of social and political destabilization through terrorist actions (Counter Extremism Project, 2024). This international expansion is part of the strategy to create a unified *"ethnically Nordic"* nation (The Guardian, ib.). The NRM movement is viewed as a significant threat to global security and, in particular, to US citizens. The United States of America has listed the NRM as a global terrorist organization because of the direct threat it poses to its citizens and to US national security. The group not only inspires violent extremism, but has also carried out terrorist attacks and actions that have endangered public safety (Ib.). The designation by the US State Department has significant implications: all of the organization's assets in the United States of America will be frozen and its members will be blocked from accessing the US financial system. This measure is a direct reaction to the NRM's history of violence and extremism, but also to the Biden administration's strategy to combat domestic and transnational terrorism with ties to white supremacist movements (Ib.).

Thus, the NRM is organized into regional divisions, with a centralized leadership and local leaders, continuing to be active and influential despite internal conflicts. The group uses social media to recruit and spread extremist messages, helping to radicalize young people and escalate violence. Although banned in Finland, the organization continues to operate under other names. Its international presence and ties to extremist groups in other countries make the NRM a significant threat to global security, including for the United States of America, which has designated the group as a terrorist organization.

CONCLUSIONS

The analysis of the activities and ideology of the Nordic Resistance Movement highlights the complexity of the phenomenon of right-wing extremism in Scandinavia and the risks it generates at the international level. Using theoretical concepts from *securitization, radicalization* and *asymmetric conflict*, the paper aims to explain

the mechanisms by which NRM has become a significant threat to regional and global security. The three theories offer complementary perspectives on the activities and impact of the NRM, highlighting the complex nature of this extremist organization.

Securitization theory – assessing the threat through the perspective of the Nordic states and the USA. Applying securitization theory (Buzan, Waever, de Wilde, ib.) helps to understand how Nordic states and US authorities came to perceive NRM as a security threat. Securitization explains how political and social issues become subjects of security through the discourses of the authorities, influencing the adopted policies. In the case of the NRM, the organization's actions, from violent attacks to extremist rhetoric, have attracted the attention of states, which have securitized this threat through formal labelling and listing the group as a terrorist organization, as the US Department of State recently did. This theory thus explains how, by formally recognizing the threat, state authorities legitimize concrete actions to counter the group's activities. Practically, securitization allows states to allocate resources and apply special measures against the NRM and its international connections, including justifying transnational cooperation in the face of a potentially destabilizing phenomenon for democratic societies.

Radicalization theory – analysis of the psychosocial mechanisms of extremist mobilization. Radicalization theory (McCauley, Moskalenko, 2008) provides an interpretive framework for the processes of attracting and mobilizing disillusioned youth within the NRM. By analysing psychological and social processes, the theory helps us understand how Norse symbols and mythology are manipulated to create a group identity that attracts supporters through a sense of belonging. These symbols not only have a cultural value, but function as tools of emotional and psychological manipulation, motivating NRM supporters to embrace a *"pure"* and heroic identity, giving them purpose and justification for violent acts. By applying radicalization theory, the study identifies the techniques by which the NRM not only recruits, but also radicalizes members, facilitating the transition from ideological support to concrete actions of extreme violence. The organization's symbols and rhetoric, based on Viking mythology, intensify the polarization between group members and the rest of society, thus supporting the logic of an inevitable conflict between *"pure"* and *"impure"* and deepening social fractures.

Asymmetric conflict theory – the strategy of destabilization and resistance to democratic authorities. Asymmetric conflict theory (Kaldor, 2006) contributes to the analysis of the tactics used by NRM to exploit the vulnerabilities of democratic societies. As a relatively small group, the NRM engages in a form of asymmetric

conflict, using violence and guerrilla tactics to undermine the democratic order and gain visibility. This theory explains the tactics by which the NRM uses isolated and well-planned attacks to destabilize governments and spread fear. In this way, the NRM manages to maximize the impact of violence despite its limited scale, turning each act of aggression into a message to intimidate and attract new supporters. Asymmetric conflict theory thus emphasizes how the NRM's decentralized structure and use of nationalist symbols contribute to the organization's survival and expansion, even in the face of restrictive measures and its designation as a terrorist organization.

The integration of these three theories highlights that NRM is not just an isolated extremist threat, but a complex, multidimensional phenomenon that requires an integrated and collaborative approach at the international level. The theory of securitization explains the state reactions and the justification of the severe measures taken by the authorities against the NRM. The theory of radicalization clarifies the attraction exerted on individuals, especially young people, who are mobilized by an identity built on the foundations of a recontextualized mythology and symbolism. Finally, asymmetric conflict theory details the strategy of destabilizing democratic institutions used by the group to maintain pressure on the state despite limited resources. NRM remains a complex threat that calls for combined and coordinated measures between national and international authorities. Only through a thorough understanding of the way these theories are applied in practice can a security framework be developed to effectively combat extremist movements of this type.

BIBLIOGRAPHY:

1. ADL (2022). *The Nordic Resistance Movement*. ADL Report, 03/21/2022, https://www.adl.org/resources/report/nordic-resistance-movement, retrieved on 3 September 2024.
2. Bjørgo, T., Ravndal, J.A. (December 2020). *Why the Nordic Resistance Movement Restrains Its Use of Violence*. Perspectives on Terrorism, vol. 14, no. 6, special issue: Restraint in Terrorist Groups and Radical Milieus.
3. Blazakis, J.M. (30 June 2024-a). *Understanding the State Department's Latest Far-Right Terrorist Designation*. Lawfare, Sunday, https://www.lawfaremedia.org/article/understanding-the-state-department-s-latest-far-right-terrorist-designation, retrieved on 4 September 2024.
4. Blazakis, J.M. (1 July 2024-b). *US's terrorist listing of European far-right group signals fears of rising threat – both abroad and at home*. The Conversation, https://theconversation.com/uss-terrorist-listing-of-european-far-right-group-signals-fears-of-rising-threat-both-abroad-and-at-home-232794, retrieved on 4 September 2024.

5. Butters, A.M. (2023). *Shades of whiteness: The appropriation of religious symbols by the Nordic Alt-Right*. Approaching Religion, 13(3), pp. 60-81, https://doi.org/10.30664/ar.131412, retrieved on 3 September 2024.
6. Buzan, B., Wæver, O., de Wilde, J. (1998). *Security: A New Framework for Analysis*. Boulder, CO: Lynne Rienner Publishers.
7. Center on Terrorism, Extremism, and Counterterrorism (18 November 2022). *Dangerous Organizations and Bad Actors: Nordic Resistance Movement*. Middlebury Institute of International Studies at Monterey, https://www.middlebury.edu/institute/ctec-publications-0/dangerous-organizations-and-bad-actors-nordic-resistance-movement, retrieved on 1 September 2024.
8. Counter Extremism Project (2024). *Nordic Resistance Movement*. https://www.counterextremism.com/supremacy/nordic-resistance-movement, retrieved on 5 September 2024.
9. Dinulescu, I. (2020). *Fanatismul religios legionar: de la apariţia în România la promovarea de către extrema dreaptă din Statele Unite ale Americii*. Top Form.
10. Kaldor, M. (2006). *New and Old Wars: Organized Violence in a Global Era* (2nd ed.). Stanford, CA: Stanford University Press.
11. Kenes, B. (April 2020). *NMR: A Nordic neo-Nazi organization with aims of establishing totalitarian rule across Scandinavia*. ECPS – European Center for Populism Studies, https://www.populismstudies.org/wp-content/uploads/2021/05/ECPS-Organisational-Profile-Series-4.pdf, retrieved on 1 September 2024.
12. Lodenius, A.L. (2020). *Framväxten av högerextremismen i Sverige*. In: Ranstorp, M., Ahlin, F. Från (31 August 2020). *Nordiska motståndsrörelsen till alternativhögern En studie om den svenska radikalnationalistiska miljön*. Centrum för Asymmetriska Hot-och Terrorism Studier (CATS). Försvarshögskolan, https://www.fhs.se/download/18.aa44b1740d51053bc784/1599031490867/Från%20Nordiska%20motståndsrörelsen%20till%20alternativhögern%20-%20en%20studie%20om%20den%20svenska%20radikalnationalistiska%20miljön.pdf, retrieved on 1 September 2024.
13. McCauley, C., Moskalenko, S. (2008). *Mechanisms of Political Radicalization: Pathways Toward Terrorism. Terrorism and Political Violence*. Vol. 20, no. 3.
14. Miller, M. (14 June 2024). *Terrorist Designations of Nordic Resistance Movement and Three Leaders*. U.S. Department of State, https://www.state.gov/terrorist-designations-of-nordic-resistance-movement-and-three-leaders-2/, retrieved on 4 September 2024.
15. Nikitins, T.J. (2020). *Sacred Symbols Becoming Battlegrounds*. In *Paganism and Its Discontents: Enduring Problems of Racialized Identity*, https://www.academia.edu/44898078/Sacred_Symbols_Becoming_Battlegrounds retrieved on 5 September 2024.
16. Pollard, J. (2016). *Skinhead culture: the ideologies, mythologies, religions and conspiracy theories of racist skinheads*. Patterns of Prejudice. Vol. 50, no. 4-5.
17. Ranstorp, M., Ahlin, F. (2020). *Executive summary: From the Nordic Resistance Movement to the Alternative Right – A study of the Swedish radical nationalist milieu*. CATS, Swedish Defence University, https://www.fhs.se/download/18.23f6da6b173f8bed598498cc/1598877052261/Summary%20-%20From%20the%20Nordic%20Resistance%20Movement%20to%20the%20Alternative%20Right%20%E2%80%93%20a%20Study%20of%20Radical%20Nationalistic%20Environments%20in%20Sweden.pdf, retrieved on 5 September 2024.
18. Ravndal, J.A. (2019). *Transnational Militancy in the Making: A Primer on the Nordic Resistance Movement and Generation Identity*. C-Rex Working Paper Series, nr. 1/2019, https://www.sv.uio.no/c-rex/english/publications/c-rex-working-paper-series/transnational-militancy-in-the-making.pdf, retrieved on 3 September 2024.
19. Rekawek, K., Finnsiö, M. (19 iulie 2024). *An Interview with Morgan Finnsiö on the Nordic Resistance Movement (NRM)*. The International Centre for Counter-Terrorism (ICCT), https://www.icct.nl/publication/interview-morgan-finnsio-nordic-resistance-movement-nrm, retrieved on 4 September 2024.
20. Riis-Knudsen, P.H. (2010). *Nationalsocialismen. Den biologiska världsåskådningen*. Nationellt motstånd förlag, https://web.archive.org/web/20110409210816/http://www.patriot.nu/files/nsdbv.pdf, retrieved on 1 September 2024.
21. The Guardian (14 June 2024). *US designates Scandinavian neo-Nazi group and three leaders as terrorists – State department says Nordic Resistance Movement, known by Swedish acronym NMR, is threat to Americans*, https://www.theguardian.com/world/article/2024/jun/14/us-nmr-terrorist-neo-nazi-group, retrieved on 4 September 2024.

THE RED AND BLUE: THE SOVIET GENERAL STAFF'S WARGAMES (1940)

Ridvan Bari URCOSTA, PhD
Strategic Studies Department, University of Warsaw, Poland
0000-0002-3675-2445 (ORCID)
DOI: 10.55535/RMT.2024.4.27

The article delves into the historically secretive realm of Soviet wargames, shedding light on two pivotal exercises conducted in 1940. These wargames, previously concealed from public knowledge, have significant implications for understanding the Soviet military strategy and the Cold War era.

By analysing archival materials and historical context, the article explores the operational-strategic doctrine of the Soviet Union, revealing insights into the military's approach to Eastern Europe.

The wargames marked a departure from traditional simulations, signalling the Soviet Union's readiness to execute both defensive and offensive operations on a continental scale. Furthermore, they laid the groundwork for subsequent military exercises during the Cold War era, shaping the course of Soviet military strategy and geopolitical considerations.

Keywords: wargames; Zhukov; Stalin; theory of war; Cold War;

INTRODUCTION

The Soviet General Staff capabilities to orchestrate and oversee extensive military campaigns in Europe played a pivotal role in shaping the Cold War-era Soviet military strategic thought pertaining to warfare on the European continent.

In the realm of Russian and Soviet military history, the tradition of conducting wargames holds significant importance. However, unlike Western countries, neither the Russian Empire, the Soviet Union, nor the Russian Federation's military tradition extensively documents or publicly discusses the outcomes of these exercises or the methodologies employed. Within the Russian tradition, the insights and strategies of the General Staff are held in high regard and often treated as sacrosanct knowledge. The Kremlin typically keeps such knowledge concealed from the public eye. Nevertheless, following the collapse of the Soviet Union, historians managed to shed light on two of the most secretive Soviet wargames conducted in 1940. It was made feasible by the opening of Soviet archives to both Western and Russian historians during the 1990s. Certain authors referenced in this discourse undertook thorough analyses of primary Russian sources pertaining to these exercises, as found within archival materials.

The objective of the article is to explore the operational-strategic doctrine of the Soviet Union, analysing the strategic possibilities available to the Soviet military command within the Eastern European theatre of war. Moreover, it seeks to trace the evolution of Soviet military-strategic thought, particularly in regard to the conduct of wargames, reaching a new historical threshold. The mentioned wargames differed from mere simulations conducted by generals aiming to integrate the experiences of the Civil War into future warfare theory. Instead, they demonstrated the Soviet Union's readiness to execute both defensive and offensive operations on a new strategic scale, spanning the entire spectrum of potential conflicts from the Baltic Sea to the Black Sea. The wargames marked the first instances of Soviet military exercises conducted at a continental level, prompting Soviet generals to contemplate strategies on a grand scale. For instance, they included simulations and military plans devised by the Warsaw Pact, such as the 1964 Soviet Plan (PHP, 2000, p. 2) for the invasion of the Western Europe.

The wargames laid the groundwork for subsequent military exercises conducted in the Soviet Union during the Cold War era. They elucidate the Soviet military's approach to Eastern Europe as a *"pred-polye"* (*"pre-field"* or *"foreground"*) zone, which, in military terminology, signifies strategic depth. In essence, the wargames designated the regions encompassing the Baltic States, Eastern Poland (including Lwow), as well as territories in Western Ukraine and Belarus, as areas of potential conflict and contention.

From a historical and geopolitical standpoint, the exercises shed light on Soviet military thought regarding the European continent in the event of conflict during the Cold War era. Furthermore, they offer insights into contemporary Eastern Europe, where Russia once again poses a security threat to neighbouring states such as the Baltic States and Poland. Paradoxically, if the Soviets conducted the wargames at the end of December 1940, the Germans just a couple of weeks ago finished *"Barbarossa Wargames"*, the simulation of the invasion of the Soviet Union. Joseph Stalin and Adolf Hitler personally followed the results of these games in their own countries. So, simultaneously, two dictators and their military leaders were deeply immersed in theoretical studies and preparations for a major conflict in the *"pred-polye"* regions. Strikingly, simultaneously the same preparations were arranged by the Americans in the spring of 1940-1941 known as the *"Louisiana Maneuvers"*.

Furthermore, the strategic significance of these wargames extends to Western military command and leadership, as both offensive and defensive operations were extensively simulated on Polish territory. Given the present circumstances, it is highly probable that the Russian General Staff is well aware of these games. In the event of conflict spilling over from regions such as Ukraine, Belarus, and other strategically vital areas in Eastern Europe, the insights gained from these two wargames, combined with lessons from the Second World War and Soviet Cold War doctrines, will hold practical importance for Russian military leadership.

For the Soviet military command and the Stavka, particularly under Stalin's leadership, these wargames represented a seminal strategic and theoretical experience that profoundly influenced Soviet military and political thought post-1945, marking the onset of the Cold War era. The Western or European theatre of war emerged as the primary focus for potential conflict with the West throughout the entire Cold War period. These wargames played a crucial role in shaping the teleological preparation for the heightened scale of military strategy required during the Cold War.

For instance, General Lieutenant A. Vladimirskiy, in his 1964 article *"Once More on the Modern Concept and Classification of Theatres of Military Operations"*, outlined the Soviet Command's perspective on theatres of war. Vladimirskiy identified seven theatres, with primary emphasis placed on the European (Western) Theatre of Military Operations. This theatre encompassed all European countries up to the Ural Mountains, Northern Africa, and the western portion of Asia Minor. The naval component extended from the Arctic to the Mediterranean. Within this theatre, Vladimirskiy delineated various strategic *"axes"*, including European territories north of a line passing through Kyiv, the Carpathians, the Alps, Toulouse, Madrid, and Cadiz. However, he underscored the utmost importance of regions such as Scandinavia, the Baltic straits zone, Central Europe, and the British Isles (*"Military Thought",* No. 2/1965; 3/1964). Consequently, these wargames served as a platform for the Soviets to develop proficiency in conducting military operations on a pan-European scale.

THE SOVIET WARGAMES ON THE EVE OF 1941

Six months prior to the outbreak of the war in 1941, the Soviet Union conducted two significant operational-strategic map-based exercises, involving the highest Command Staff of the Red Army, held at the General Staff of the Red Army. The main hero of the wargames, Marshal of the Soviet Union G.K. Zhukov, argued that: *"The military-strategic game mainly aimed to test the reality and expediency of the main provisions of the coverage plan and the actions of the troops in the initial period of the war."* (Жуков/Zhukov, 1986, p. 239).

It should be noted that the General Staff regularly conducted military-strategic wargames. For instance, from April 19th to April 25th 1936, wargames were organized. The primary focus of the hypothetical conflict was the area along the Belarusian-Polish border. There was even consideration given to the possibility of engaging in a major battle against a potential Western adversary within Belarusian territory. Actions in the Ukrainian and Baltic war theatres were deemed secondary in importance during these exercises (Захаров/ Zakharov, 1989, p. 93).

In the Belarusian theatres the *"Red"* concentrated 1250 aircraft and five armies. The Soviet General Staff paid a lot of time and effort to this wargame and, according to Chief of the General Staff (1960-63) Matvey Zakharov, many calculations that were analysed during the game were predicted when the real war started. But some egregious errors were made due to approaches that relied on the old premises which were built during the First World War and the Civil War. The number of forces

was more or less equal, the main forces of the *"Red"* already were deployed to the border; the command had not anticipated that the *"Blue"* might faster deploy forces to the border and make the first attack. Moreover, the factor of surprise attack had not been examined. Despite objective old assumptions, the wargame triggered the process of reflection and modification of many retrograde theoretical assumptions. In 1937, the General Staff initiated a new wargame *"Army offensive operation in the initial period of the war"* which tried to tackle many theoretical problems which emerged in 1936.

In Soviet historiography, the subject of wargames conducted before the German invasion of the USSR was tightly controlled by Soviet propaganda, and Soviet historians had only a partial understanding of these exercises. Comprehensive research on this topic only began to emerge in the 1990s, following the collapse of the Soviet Union. Even when some authors in the Soviet Union wrote about this topic, the information was carefully integrated into the Soviet narrative of the country's and army's defensive preparedness for a potential war, while concealing the offensive nature of the exercises (Бобылёв/Bewitelyov, 1995, No. 5).

It was an established Soviet tradition to conduct the most significant military wargames and discussions in the final days of the year. Between 23 and 31 December 1940, such activities were particularly crucial. At that time, the wargames and meetings took on added importance due to the recent conclusion of the Soviet-Finnish War in March 1940 and the onset of the Second World War with the occupation of Poland and France. Additionally, the impact of the blitzkrieg tactics employed by the German Armed Forces in Poland and France was keenly felt during the wargames. The Soviet generals were deeply impressed by the rapid and decisive nature of these German attacks in both countries.

In his 1986 version of *"Memories and Recollections"*, Zhukov recounted that, at the end of September 1940, he received a message from the General Staff indicating that a meeting of the highest command staff of the army would be held in Moscow in December, directed by the Central Committee of the party. He was assigned the task of delivering a report on the topic *"Characteristics of a Modern Offensive Operation"* for the planned large-scale operational-strategic games, where he was to represent the *"blue"* side. Zhukov recalled in his memoirs that every general was aware that they were preparing for a potential conflict *"against the strongest army of the West"*. According to Zhukov's recollections, Stalin invited him and Timoshenko to his office to discuss the upcoming wargames. Zhukov acknowledged that the games held significant dramatic and symbolic meaning

for the Soviet leadership, as they revealed all the concerns he had, which later became tragically apparent in June 1941. Following the conclusion of the games, Stalin summoned the generals to the Kremlin. He expressed disappointment at the news of the *"Red"* side's defeat and added: *"Let us not forget that in war, it is not just about numerical superiority, but also about the art of commanders and troops".* (Жуков/Zhukov, ib., p. 240). To Pavlov's defence speech during the meeting, Stalin stated that *"The commander of the military district must possess the art of war, capable of making the right decisions in any circumstances"* (Ib., p. 241). According to Stalin, the victory in the future war will be on the side of those who possess more tanks and higher motorization of troops (Ib., p. 242). Such philosophical confession was possible from Stalin quite often. For example, on 14 April 1940, he delivered a speech in front of the General Staff and lamented that the Red Army lack of agility and manoeuvrability were not properly adopted to the changing warfare in Finland. He added: *This was the main factor preventing our troops from quickly adapting to the primary conditions of the war in Finland. They failed to understand that it was not just a military walkover but a real war. The mentality that our army is invincible, coupled with the boasting, which is rampant among us – and the most ignorant people are usually the biggest boasters – must end. We need to permanently get rid of this boasting. Our people need to be drilled with the understanding that no army is invincible. We should remind them of Lenin's words: armies that have been defeated or have suffered losses often fight very well afterward. Our people, from the command staff to the regular soldiers, must understand that war is a game with some unknowns, where defeats can happen. Therefore, we must learn not only how to advance but also how to retreat. The most important thing to remember is Lenin's philosophy.*

It remains unsurpassed, and it would be good if our Bolsheviks grasped this philosophy, which is fundamentally different from the naive belief that our army is invincible, has everything, and can overcome anything. We must abandon this mindset of ‹throwing our hats over the problem› if we want our army to become a truly modern force. What prevented our army from quickly adapting and preparing for serious warfare, not just a walkover? What hindered our command staff from restructuring their approach to fight the war not in an old-fashioned but in a new way? Bear in mind that, throughout the entire existence of Soviet power, we have not yet fought a real modern war. Minor episodes in Manchuria, Lake Khasan, or Mongolia are trivial; they are not wars but isolated skirmishes in small, well-defined areas. Japan was afraid to start a war, and we did not want it either,

and the small skirmishes demonstrated that Japan failed". (Документы, 1941, год: Кн. 1, Documents: Year 1941, p. 602). From the General Staff, during the wargames, he will demand exactly this new military philosophy that would prepare the Red Army for the future warfare.

Despite the advent of Perestroika in 1986, the full version of Zhukov's memoirs was not published at that time. It was not until 2002 that the complete memoirs, including previously censored sentences from the Soviet era, were finally released. In these memoirs, Zhukov reveals details that were previously censored. Specifically, Zhukov writes about the moment during the wargames when *"…our military theoretical science did not thoroughly consider the issues of strategic defence, mistakenly deeming it less important"* (Жуков/Zhukov, 2002, p. 198). He regrettably confesses that the Soviet strategic thinking has not reached proper level of understanding of the modern warfare. In relation to this aspect, he writes: *"The thing is, until 1940, our military-political leadership lacked a solid understanding of the significance of the methods and forms of deploying large tank and mechanized units like corps-army in modern warfare."* (Ib., p. 199).

In 2005, the Russian historian Vladimir Sherstnev provided a more detailed analysis and evidence about this event in his book. According to Sherstnev, during the meeting with the commanders in the Kremlin, Stalin was displeased with the tone of the outcomes presented by the General Staff regarding the wargames. The final conclusion suggested that Soviet divisions were much stronger than the German ones. Stalin increasingly realized that the General Staff was making subjective assessments of both its own troops and the potential adversary. Sherstnev noted that, in his speech, Stalin highlighted how the war in Europe had revealed that the Germans initiated military actions with pre-mobilized and deployed forces, concentrating the full might of their tank and air forces in the initial strike. Stalin criticized the military leadership for failing to comprehend the new operational art demonstrated by the Wehrmacht in Poland and the West. By conducting operational-strategic games based on their prepared tasks, the General Staff was, in Stalin's view, improperly preparing the command of the districts and armies to repel aggression, potentially even criminally so. The Finnish war further exposed the unpreparedness for war among commanders at all levels, and Stalin lamented that the General Staff, as the *"brain of the army"*, still lacked measures to successfully repel a sudden powerful strike and did not know how to counter the enemy's blow with the full force of the wartime army using the peacetime army.

Stalin demanded that the General Staff should urgently develop and present a new mobilization plan to the government and make adjustments to the operational plan in line with the changed military-political situation worldwide. He emphasized the need to expedite the equipment of the Air Force and troops with planes and tanks and sharply criticized the views of some individuals who underestimated motorization (Шерстнев/Sherstnev, 2005, pp. 171-173).

Finally, Stalin concludes the following: *"For several years the Central Committee of the party and the government literally ‹imposed› on the leadership of the People's Commissariat of Defence the idea of the necessity of creating large mechanized tank formations. But the People's Commissariat of Defence showed some remarkable timidity in this regard. (...) Kulik defends a large 18,000-strong division on horse-drawn transport; he opposes the mechanization of the army. The government is pushing for the mechanization of the army, introducing engines into the army, while Kulik opposes engines. It is as if he were advocating against tractors and combines, defending the plough and the economic backwardness of the countryside. If the government had taken Kulik's point of view, say, during the years of collectivization of agriculture, we would have been left with individual farms and the plough".* In the same speech, it was emphasized: *"Modern warfare will be a war of engines: engines on land, engines in the air, engines on water and underwater. In these conditions, victory will belong to those who have more engines and greater reserves of power!" And he concluded his speech by stating that it is not armies that fight, but economies. The level of a military leader's art is ultimately determined by the economic resources and capabilities of the country."* (Ib., p. 174).

RED ARMY'S DECEMBER 1940 COMMAND STAFF MEETING: DOCTRINAL SHIFTS IN SOVIET MILITARY DOCTRINE

In December, a meeting of the senior command staff of the Red Army was held in Moscow, which was attended by the heads of the People's Commissariat of Defence and the General Staff, heads of main departments, inspector generals of military branches, commanders, members of military councils, chiefs of staff of military districts and armies, heads of military academies, commanders of some corps and divisions, and other officials – more than 270 people in total. This representative meeting and the subsequent operational-strategic games on the maps completed the operational training of the Red Army command staff in 1940 (БобылевП.Н, Военно-Исторический Журнал/Military-Historical Journal, 1993, p. 9).

At the first meeting the participants discussed interesting issues, namely:

1. *"The results and tasks of the combat training of the Ground Forces, the Air Force and the operational training of the highest command personnel"* (speaker, Chief of the General Staff of the Red Army, General of the Army K. A. Meretskov);
2. *"Character of the modern offensive operation"* (speaker, Commander of the Kyiv Special Military District, General of the Army G. K. Zhukov). Zhukov, in his report before the games, presented his assessment of geostrategic situation in the world and in Europe and outlined importance of the development of the cutting-edge military technologies (first of all, the tanks, artillery and aviation), which make the war faster and more fundamental than it was before. However, he outlined that only Nazi Germany had demonstrated its ability to conduct deep operations and operational art (Русский архив/Russian archive, 1993). In this address in front of the Soviet military leadership Zhukov presented his maturity as commander and his intellectual preparedness to conduct 20th-century grand-scale military operations. For example, Zhukov stressed that *"In the conditions of our Western theatre of military operations, a large-scale offensive operation with a strategic objective, it seems to me, should be conducted on a broad front, at least on a scale of 400-450 km"*. Such logic is certainly quite close to the Cold War military doctrine of the Soviet Union;
3. *"Air Force in offensive operations and in the struggle for air dominance"* (reported by Chief of the Main Directorate of the Red Army Air Force, Lieutenant General of Aviation P. V. Rychagov). Rychagov's ideas found positive response during discussions. Especially among the main tasks of aviation, he particularly emphasized the task of achieving strategic and operational air superiority (История военной стратегии России/History of Russian Military Strategy, 2000, p. 244);
4. *"The nature of a modern defensive operation"* (speaker, Commander of the Moscow Military District, General of the 4th Army, Tyulenev);
5. *"The use of mechanized formations in a modern offensive operation and the introduction of a mechanized corps into a breakthrough"* (speaker, Commander of the Western Special Military District, Colonel General of Tank Forces D.G. Pavlov);
6. *"Combat of a Rifle Division in offensive and defensive"* (Rapporteur, Inspector General of the Red Army Infantry, Lieutenant General A. K. Smirnov).

It was not coincidental that all reports had a theoretical nature; the recent geopolitical situation underscored the necessity for new military theories and a reassessment of the experiences gained by Soviet generals on the battlefields of the First World War and the Civil War. Furthermore, the meeting revealed underlying problems within the community of Soviet military intellectuals. Many of those who had developed the renowned theories of *"deep defence"* and *"deep offense"* operations had either suffered or were killed by the Soviet regime at the end of the 1930s.

During the meeting, many generals acknowledged that Soviet military schools were in a state of deep crisis and that serious studies of recent European wars experiences had not been undertaken. Interestingly, it was recognized that the experiences of Soviet officers in the wars of the 1910s and 1920s were not directly applicable to the Soviet-Finnish War and, especially, to the contemporary wars being waged by Germany in Europe. Ironically, even within such closed meetings of high command, there were individuals advocating for strict adherence to ideological postulates and cautioning against overestimating Germany's successes in Europe.

It appears that the Soviet generals were indirectly inclined to discard the last remnants of doctrinal experiences from the Civil War era and transition contemporary military thinking towards the scale and scope of modern industrial warfare characteristic of the 20th century. These wargames can be viewed as the initial strides toward a conventional, non-nuclear form of warfare akin to what would later emerge during the Cold War. Upon careful examination of these reports, it becomes evident that the generals were discussing the future of warfare. They articulated the necessary steps to modernize the Red Army and bring it in line with contemporary standards of warfare.

The generals did not directly discuss the possibility of war between Germany and the USSR, but it was implicitly acknowledged as a theoretical possibility in the statements made by the speakers. The ultimate decision reached was to address all the Armed Forces discrepancies within the next six months. Furthermore, there was a regrettable acceptance of the fact that the army was not prepared for war and that its combat readiness was deteriorating. However, the primary issue identified lay in the low qualifications of the vast majority of the command staff of the Red Army (Ib., p. 13). Nevertheless, there was unanimous agreement among the participants that the military literature and documents pertaining to the art of war must be revised and aligned with the principles of the new warfare theory.

An intriguing discussion ensued regarding the issue of air control and dominance among the Soviet generals. Two distinct groups emerged: the first group favoured the German approach of launching massive attacks on enemy airfields, while the second group believed that success in air operations primarily depended on defeating and suppressing the enemy in air battles.

Additionally, General I.V. Tyulenev, in a report on defence issues, was compelled to acknowledge: *"... we do not have a modern substantiated theory of defence, which could be opposed to the modern theory and practice of a deep army offensive operation."* (Ib., p. 14). He delineated the fundamental principles for preparing and executing a defensive operation, emphasizing the necessity of establishing a comprehensive defensive system within the operational framework. This system should be capable of repelling large-scale tank assaults, withstanding aerial bombardments, and safeguarding personnel and firepower from enemy artillery barrages.

Regarding the role of tanks, the Soviet generals concurred with the German perspective, deeming tanks to be pivotal for success in warfare. Sergey Bobylev, a Soviet general and historian, criticized the Soviet command for neglecting to study and analyse crucial strategic issues during such an important meeting. He highlighted the oversight in addressing topics such as strategy, strategic defence, and the initial period of war, the absence of which became apparent in the early days of conflict (Ib., p. 15). Famous Russian military thinker Gyorgy Isserson came under attack during this period, particularly due to his book *"The New Forms of Combat"*, published in 1940. The book, which analysed the German-Polish War, posited that future wars would not have an initial stage but would instead commence with all available and deployed forces. Despite Isserson's assertions, none of the Soviet generals challenged this criticism. On the contrary, the Soviet command viewed Isserson's ideas as speculative and unsubstantiated.

The first-time decision to conduct the wargames was made in October 1940. The goals of the first wargames (December) were the following (БобылевП.Н, Военно-Исторический Журнал/Military-Historical Journal, 1993, No. 7, p. 14):

1. Give practice to the high command:

a) in organizing and planning a front-line, army operation, its combat and material support in the full depth;

b) in the command and control of the operation, and organization and ensuring the interaction of the armed forces and combat arms and rear management;

2. To work out and master the basics of a modern offensive operation of the front and the army, in particular:

a) organization and methods of breaking through fortified areas with overcoming barriers strongly developed in depth;

b) forcing a large river barrier;

c) organization and conduct of an anti-amphibious operation in order to prevent the landing of the sea and air assault forces;

d) organizing and ensuring the release of a large airborne assault force;

e) introduction of cavalry-mechanized groups into the breakthrough;

f) interaction with the navy.

To the wargames in 1940-1941, the Soviet command already acted as a system, with the participation of the Minister of Defence, heads of the General Staff, their deputies, and the heads of the armies. In general, were involved 32 people plus 55 technical workers (Захаров/Zakharov, ib., p. 194). On 23 June 1941, the Main Military Council of the Red Army was abolished and the Stavka of the Supreme High Command (Stavka VGK, SVGK) was established. Stavka was an extraordinary body of supreme military command that exercised strategic leadership over the Soviet armed forces during the Great Patriotic War. Thus, something like an improvised Headquarters of the Supreme Command (Stavka) was created. During this period, wargames became a focal point for discussions between commanders and Stalin himself. Stalin held the belief that Germany's primary offensive thrust should target Ukraine rather than Belarus. It was based on Germany's perceived strategic imperative to control Ukraine, particularly the Donbas region and the Caucasus oil fields. Stalin predicted that without access to these vital regions, Germany would be unable to sustain a prolonged war effort (Ib., p. 179). This assumption came from general assessments of the geopolitical situation in Europe, Moscow considering that the southern front is a priority for Germany.

Boris Shaposhnikov, the Head of the General Staff, added to this construct the assumption that the zone from the Baltic States to the Carpathians and the Bug River must be a so-called *"pre-field or foreground" ("pred-polye")* or *"zone of the fence"* with the depth up to 300 km. Above all else, these areas for the Soviet command were lost areas, hence they inevitably will be given to the enemy's control (Ib., p. 183). But Zakharov had doubts regarding Shaposhnikov's authorship of this plan.

Another significant revelation from these wargames was the strategic disadvantage faced by the Soviet Union compared to the *"Blue"*, representing Nazi Germany. According to Russian military historian Alexey Gayveronsky, the Soviets

were keenly aware of this imbalance. He refers to two notes compiled by the People's Commissar of Defence, General Timoshenko, and the Chief of the General Staff (Shaposhnikov, Meretskov, and Zhukov), on 19 August and 18 September 1940, as well as on 11 March and 15 May 1941. The notes proposed two courses of action against the Germans. One option was to deliver a decisive blow by the main forces of the Red Army to the north of Brest, aiming to crush the enemy on the Warsaw direction and open the road to Berlin. The other option was to strike powerfully towards Krakow and Breslau in the south, aiming to cut off Germany from Romanian oil supplies and *"decisively influence the Balkan countries regarding their participation in the war".* The January manoeuvres appeared to test both options, with the *"southern"* approach ultimately taking precedence. But the notes emphasize that *"Germany keeps its army deployed and mobilized, concentrating the forces necessary for a strike against the USSR within 10-15 days".* Meanwhile, the Soviets complete the strategic deployment on the 30th day from the start of mobilization (Гайворонский/Gayveronsky). According to Gayveronsky, exactly the 15-day advantage of the Germans in the strategic deployment played its tragic role in the war.

THE LAST PRE-WAR OPERATIONAL-STRATEGIC WARGAMES OF THE SOVIET UNION

In January 1941, the situation forced the Soviet Command to take the wargames more than simply theoretical routine, but as the projection of the real war. Escalation took an irreversible character in Europe. The second operational-strategic wargames took place from 2-6 January and 8-11 January 1941, but they differed in geographical conditions compared to the areas of Belarus or Western Ukraine. However, a significant portion of the frontline still encompassed Belarus, Ukraine, and Moldavia. In this iteration, the primary battles during the initial stages of the war were anticipated to unfold in the territories of Eastern and Central Poland. In 1965, Marshal of the Soviet Union A.M. Vasilevsky, who played a pivotal role in the inception of these planning exercises, remarked on their significance: *"In January 1941, when the proximity of the war was already felt quite distinctly, the main points of the operational plan were tested in a strategic military game with the participation of the highest command of the armed forces".* (Белоусова З.С./ Belousov Z.S., 1992, No. 6. p. 9).

The plot of the game. The *"Blue"/"Western"* team managed to deploy and concentrate the forces near the borders of the *"Red"/"Eastern"* team faster

that the *"Red"*. The Blue team created four fronts from the Baltic to the Black Sea and, on 15 July 1941, went on the offensive with two northern fronts. The main *"Western"* blow entailed two southern fronts (160 divisions) in the strip south of Brest in the direction of Vladimir-Volynsky, Tarnopol. Near Belarus were concentrated 60 divisions in the first echelon. They, without waiting for the full concentration of all forces, went over to the offensive in order to ensure the actions of neighbouring fronts in the main direction; striking from the regions of East Prussia in the direction of Riga and Dvinsk (Daugavpils), and from the regions of Suwalki and Brest-Litovsk to Baranovichi had the goal of reaching the front of Baranovichi, Dvinsk, Riga by 15 August. The offensive of the *"Western"* ground forces was supported by powerful air force. In the coastal direction, the troops interacted with the fleet.

Unable to hold back the pressure, the formations of the North-Eastern Front (Red) began to withdraw to a pre-prepared line of defence with a widely developed system of fortified areas. According to the plan, the Red, after regrouping, had to organize the counteroffensive operation. The Red managed to withstand the attacks of the Blue team in the Baltic Sea.

As Zakharov wrote, when drawing up game plans, the strategic situation was based on the expected events that could unfold on the western border in the event of an attack by fascist Germany on the Soviet Union.

The goals of the wargame were:

1) develop and master the basics of modern defensive and offensive operations;

2) give practice to the highest commanding staff in organizing and planning front-line and army operations, in command and control and organizing interaction between the main branches of the military and the Navy;

3) work out the following issues: defence of the state border in the event of an attack by superior enemy forces; withdraw to a prepared defensive line; conduct private operations with the aim of defeating the enemy in a frontier battle; overcome the foreground; mastery of fortified areas; break through the defensive field line of the enemy; organize the pursuit of forcing by the cavalry-mechanized army of the river, as well as mountain passes;

4) study the Baltic and Southwestern theatres (Poland and Ukraine) of operations (Ib., p. 195).

Regarding the *lessons* of the first game, there were the following conclusions:

1) The fortification systems are not enough in the new wars, they simply can be circumvented, but in some cases, the modern armies still must storm

the fortifications in order to continue their advances deeper into the enemy's territory;

2) One should strive to inflict the greatest damage on the attacker with firepower, not allowing the defeat of one's troops in parts in front of fortified areas.

3) It is also dangerous to leave the Suwalki-ledge, it is better to keep it behind you, so that in the future, with simultaneous strikes from the ledge from the Brest-Litovsk region to Baranovichi, isolate the entire main grouping of the Northwestern Front;

4) The playing parties did not organize a clear interaction of sea forces with land forces.

Thus, the results of the first game showed that the operational-strategic outlook of many top-level commanders was far from perfect and required further painstaking and persistent work in honing the art of command and control of large units, deep assimilation of the nature of modern operations, their organization, planning and consistent implementation on practice (Ib., pp. 197-201).

The second round of the games failed to adequately incorporate border changes, with players adhering to the pre-Molotov-Ribbentrop Pact borders. Additionally, the game overestimated the Red team's defence capabilities in comparison to the potential of the Blue team. The game's designers relied solely on the provisions articulated during the 1940 December meeting of senior command personnel, thereby neglecting the impact of new geopolitical realities near the Soviet borders. Moreover, the structure of the armies was rigid and inflexible, lacking integration of the regional and geographic specificities of different war theatres.

According to Soviet/Russian historian Pavel Bobylev the goals of the second war games were the following:

- To study and master the basics of the modern offensive operation of the front and the army;
- To master and work out the basics of conducting defensive operations in the conditions of a mountain theatre and in the defence of large river barriers;
- To explore the Southwestern theatre of operations;
- To give practice to senior command personnel in assessing the situation and making decisions in difficult conditions, in organizing, planning and logistical support for front-line and army operations, as well as in the field of driving large operational and, above all, mobile formations in cooperation with aviation;

- To achieve understanding and unity of views on the conduct of a modern offensive operation with the massive use of artillery, tank formations, and air forces (БобылевП.Н, Военно-Исторический Журнал/Military-Historical Journal, 1993, No. 7, No. 8, p. 28).

In the second game of the same cycle, the Blue team concentrated its forces near the Soviet borders with the intention of launching a southern-directed offensive from Lublin down to the Black Sea. The primary engagements occurred in Eastern Poland. By advancing on two fronts – the Southeastern and Southern Fronts – in the general direction of Proskurov/Płoskirów, the Blue team aimed to encircle and eliminate the Lwow-Ternopil grouping of the Red forces.

Subsequently, they planned to advance towards Odessa, Khmelniki, Shepetovka, and the Sluch River. The naval forces of the Blue team were tasked with departing the Mediterranean Sea by 8 August and overcoming the resistance of the Red naval forces by 10 August. Their objective was to break the Red blockade in the Bosporus and establish dominance in the Black Sea, thus providing support to the armies of the Southern Front along the coastal direction. In both scenarios, the Soviets considered the possibility of launching counteroffensives and even offensive operations in certain theatres.

The initial situation in this game looked like this: the Blue in alliance with the *"Southwestern"* and *"Southern"* began a war against the *"Red"*, going on the offensive with two fronts – South-Eastern and Southern but at different times.

The Southeastern front began hostilities on 1 August 1941, against the Lwów-Ternopil grouping of the Red, however, at the line of Lwów, Kovel was met with a strong resistance of the Red and, having lost up to 20 infantry divisions, by the end of 8 August, withdrew to the previously prepared line of Starina, Grybów, Tarnów, Dunaetsand Vistula Rivers. The southern front went on the offensive on 2 August, in the Proskurov direction, from Romania. Its formations broke through the defences of the Red and, developing success, by the end of 8 August, they reached the Dniester River, crossing it in the areas of Kalyus, Komarovka and Melnitsa-Podolskaya. The common task of the two fronts was to encircle and destroy the enemy in the area of Kamenets-Podolsky, Kovel, Lublin, and Rzeszow and reach the Odessa, Vinnitsa, Shepetovka, Sarny fronts by 10 September.

The task of the Southwestern Front of the Red team (under the leadership of Zhukov) was to cover from the west along the Vistula River, with the main forces to destroy the *"southwestern"* and *"southern"* (Blue) on their territory and by 16 September, to reach the front of Krakow, Budapest, Timisoara, Craiova.

In the legend was indicated that the Red is facing problems with the numbers of infantry divisions and mechanized brigades. The biggest mistake of the Blue in this game, according to Bobylev, is the refusal of the Blue's command strike on the supply lines of Zhukov's army which stretched from Lwów to Kovel. Instead, the Blue attacked only Lwów and it allowed Zhukov to continue the counteroffensive operation on the territory of Central Poland. G.K. Zhukov began a major operation in the Budapest direction with a depth of up to 300 km. A strike on Budapest split the common front of the coalition of opponents, cut off the Blue from their allies, and ensured the final defeat of the *"southwestern"* and *"southern".* Thus, the *"victory"* in the second game was on the side of the Red. In general, according to the results of both games, success was achieved by the side whose troops were commanded by G.K. Zhukov.

Miscalculations, according to Zakharov, were also made at the games with the creation of an advantageous aspect ratio – an important factor in the preparation, conduct, and successful completion of any operations. The preponderance of infantry forces in both the first and second cases turned out to be on the side of the enemy. In particular, in the first game, this circumstance allowed the *"Blue"* to create a large grouping on their left flank to strike in the direction of Riga, Dvinsk, successfully solve this problem and win the operation. The creators of the game explained this miscalculation as follows: when developing the task, they proceeded from the fact that Soviet divisions were supposedly one and a half times stronger than the German ones, and therefore, with a smaller number of formations, the advantage in manpower and equipment was on their side. Thus, the General Staff believed that the enemy had no numerical superiority. Such a biased interpretation of this crucial issue was condemned as unfounded.

In this regard, Bobylev added that the level of an operation that was unfolding in the southwestern direction during the second game exceeded in its scope the operations of the first game and was not inferior to the operations of the Second World War (and in some respects even surpassed them). For example, the operations, which were undertaken by Zhukov, say exactly about such a level because Zhukov with successful counterattacks took Krakow and furthermore moved in the direction of Budapest.

The Soviet general and historian Bobylev argues with Zakharov and says that he was the first who in detail described the wargames, but he made many key errors.

Bobylev highlights that it was also supposed to study the Baltic theatre of operations and East Prussia, to get acquainted with the basics of a defensive

operation. The core positions in the wargames were given to the head of the military western districts because in case of war they had to take major responsibility, especially during the first days of the war. Thus, Moscow prepared for the offensive operation in Eastern Europe. It was planned to get acquainted with questions of defence only to the extent that they arise in the course of the case. The priority was the theoretical issues of attack, not the defence. As a zone of war was chosen the space between the Baltic and the Black Seas. In the General Staff, all arrangements were made under time pressure because in the autumn of 1940 the geostrategic situation changed and the Soviet command did not know the direction of the main attack of Germany (Belarus or Ukraine). In that period, it was made the decision to consider the main strike from Brest to the Black Sea, not from the territories of Eastern Prussia.

Bobylev writes that both games were held in three stages, at each of which the participants, in accordance with the tasks and received introductory decisions, made decisions and executed directives, combat orders, operational reports and other documents in writing, and ended with a decision on the situation by the end of the third stage. The generals from the Red team got information that the Blue (Western) already deployed forces to Soviet borders and concentrated from Dęblin to the Baltic Sea 60 divisions, but closer to Ukraine 120-150 divisions.

The group of armies northern of Dęblin did not wait for the full concentration of their troops, in the interests of the main attack, they went on the offensive (on 15 July) with the task of defeating the Belostok-Volkovysk and Kaunas groupings of the *"Red"* and by the end of 15 August to reach the front of Baranovichi, Dvinsk, Riga. Eastern Prussia was the main centre of gravity for the attack on the Soviet position in the Baltic and Belarus. There the *"Red"* arrested the *"Blue"* attack and turned with the 50 divisions to counterattack. The North-Western Front of the *"Red"*, having repelled the offensive of the *"Blue"*, by 1 August reached the state border line and received the following task: to defeat the *"Blue"* in East Prussia and by 3 September 1941, to reach the river Vistula from Wloclawek to the mouth.

Concurrently, the Blue did not achieve success in its march on Leningrad, instead, according to the game the Soviets managed to repel the Blue. As Bobylev wrote, the assignments for both the *"Western"* and the *"Eastern"* also described the situation in the Baltic Sea. Detailed reference information was attached to the assignments: tables of combat strength, statements of troop supply on the eve of operations, plans and tables of troop regroupings, information on the capacity

of railway sections etc. The decisions of the parties based on those data predetermined the course of the game (Ib., p. 16).

Here I would like to cite several paragraphs directly, without changes, because it has practical importance in case of war in the zone of the historical regions: Prussia, Podlachia, and Suwalki. For any future war in Eastern Europe, the commanders will face similar challenges as their predecessors faced when they fought in these territories. The Russo-Ukrainian War shows that both sides have been obliged to learn and study the logic of the decisions of commanders who fought in the areas of the old Wild Steppe. It is maybe the most important part of the wargames:

The commander of the North-Eastern Front of the *"Western"* (Blue) (his duties in the game were performed by G.K. Zhukov) decided: firmly rely on the fortified areas and borders of East Prussia, to prevent the enemy from invading the territory of the *"Western"*, but at the same time continue to concentrate suitable reserves, simultaneously by inflicting short blows with the aim of exhausting the enemy, in order to go over to the general offensive on 10 August 1941.

The presence of powerful fortifications, as well as a large number of roads that made it possible to quickly manoeuvre the forces and means, gave the *"Western"* the opportunity to hold the occupied lines (in particular, important in the operational direction Suwalki ledge) until the reserves approached. Thus, until 10 August, the North-Eastern Front (10th, 9th, and 8th armies) planned to conduct a defensive operation; then it was supposed to attack to a depth of 120-130 km to the line Bialystok, Volkovysk, Orany, Shavli lasting 12-13 days. During the next stage of the offensive, it was planned to fulfil the task set by the *"Western"* headquarters to reach the Minsk, Dvinsk, and Riga fronts by 5 September.

The commander of the North-Western Front of the *"Eastern"* (General of the Tank Forces D.G. Pavlov), when making a decision, proceeded from the fact that, by 1 August, the front had a general superiority over the enemy, and therefore, it was necessary to defeat the *"Western"* before the approach of their reserves, which, according to the assumptions of the command of the North-Western Front, could happen on 10-12 August (then the enemy could go on the offensive).

It was expected that relying on the Suwalki fortified area, the main forces of the *"Western"* would strike in the direction of Dvinsk and Riga, and simultaneously from the regions of Suwalki and Brest – to Baranovichi. The most dangerous was considered a strike from the Suwalki area to Grodno, Volkovysk with access to the rear of the left-flank armies of the North-Western Front. Therefore, it was considered expedient to start the offensive no later than 5 August, in order to break

up the forces of the *"Western"* on the first defensive line before approaching and putting their reserves into the battle.

The operation of the North-Western Front (Red) was presented to his headquarters in the following form:

- the first stage (1-5 August) – preparation for breaking through the first defensive line; the task is to destroy the enemy on the eastern bank of the Neman River, with private operations of the 1st Army, and prepare to cross it. The 14th Army and the 19th Army in the Suwalki area approach closer to the first defensive line and prepare for its breakthrough;
- the second stage (6-11 August) – forcing the Neman River and breaking through the first defensive line on the rest of the front with the destruction of the enemy on the eastern Masurian Lakes; breakthrough depth – 40-45 km;
- the third stage (12-15 August) – regrouping and preparation for breaking through the second defensive line;
- fourth stage (16-22 August) – a breakthrough of the second defensive line; breakthrough depth – 40-50 km;
- the fifth stage (23 August-3 September) –the development of the offensive operation, the defeat of reserves (reinforcements), and the establishment of the access to the Vistula River; advance depth – 180-200 km. The total depth of the front-line operation was 250-300 km according to the plan.

Many tasks which were indicated by the Soviet Command (Red) initially were fulfilled. The Soviets even managed to cross the Neman River and reach the echeloned defence of the Blue. Zhukov (Blue) organized effective defence and successfully used massive fortifications. As a result, the Soviets had been facing enormous resistance and losses. The fact is that, by decision of the commander of the North-Eastern Front of the Blue, on the right flank of defending the 9th Army of the *"Western"* in the area of Eastern Prussia, it was concentrated a large grouping of troops (four armies and one mechanized corps, two tank divisions, and four tank brigades). Such significant force was possible to create mainly due to the reserves that arrived on the front. On the morning of 12 August, this powerful group went on the offensive in the direction of Grabowo, Stawiski, and Lomrza. As result, the Red's front was broken. Zhukov with this manoeuvre changed completely the situation on the front and managed to achieve superiority of manpower and mechanized groups.

The Blue team won the initial stage of the war. Thus, the Red failed to encircle and defeat the East Prussian grouping of the Blue. Moreover, a significant number

of their own forces were under the threat of encirclement and defeat. Moscow was not satisfied with the results because they contradicted the official ideology (the Red could not be defeated) and this objective game demonstrated that all military calculations of the Soviet military command were based on the wrong theoretical grounds. However, despite all the mentioned aspects, it was the last important theoretical game for the Soviet military command before the German invasion of the USSR in June 1941.

After the end of the games, Stalin invited the generals who actively participated in the games to the Kremlin. Stalin was deeply dissatisfied with the fact of the Red's defeat and consequently appointed Zhukov as a Commander of the General Staff. Stalin reportedly stated after the games that, in reality, the Soviet command did not have a real head of the General Staff. Moreover, during the discussion, Zhukov drew attention on the fact that *"in Belarus, fortified lines (URs) are built too close to the border and they have an extremely unfavourable operational configuration, especially in the area of the Bialystok ledge. This will allow the enemy to strike from the area of Brest and Suwalki to the rear of our entire Bialystok grouping. In addition, due to the small depth, the URs cannot hold out for a long time, as they are shot through by artillery fire."* (Жуков/Zhukov, ib., p. 241).

Zhukov suggested to move to the east the fortifications from the Belarus border up to 100 km and create more secure strategic depth. Russian historian Sokolov criticized Zhukov because, in his opinion, the Soviet command prepared the offensive operation to invade the Western Europe and the defensive rhetoric as only a trick (Соколов/Sokolov, 2000, p. 199). Yet another Russian historian, Metukhov, writes that the success of Zhukov in Ukraine and Southern Poland during the second round of games and the defeat of the Red in the Northern Theatre (Belarus and Eastern Prussia) determined the decision of the Soviet Command to refuse to use Belarus as the zone of future offensive operations (Мельтюхов/Meltukhov, 2000).

Finally, I would like to refer to Professor Cynthia A. Roberts, who provided a quite objective and rational assessment of these wargames. She wrote the following: *"Despite the two very different results for the ‹Eastern› or Soviet side in the games, both exercises were similar in their failure to consider realistic contingencies. Most important, the war games did not employ scenarios which fully embodied the experience of German operations in the West, thereby avoiding the importance of surprise, mass and striking power in German Blitzkrieg. Nor did the games reveal any recognition of the impediment that the Red Army, like its tsarist predecessor, was slow, ineffective and cumbersome. Germany's defeat of France and the Soviet*

Union's pyrrhic victory in the Winter War had demonstrated that the Red Army was unprepared for modern warfare; nevertheless, Soviet commanders continued to adhere to an obsolete doctrine which assumed a slower than realistic initial rate of advance for the enemy and the ability of the Soviet defender to stop the invader near the frontier and push him back across the border. In the war games, therefore, the standard conceptualization of the initial period remained unchallenged. [...] However, strong resistance mounted by the defender near Lvov, followed by counter-offensives, destroyed 20 enemy infantry divisions within a week. This orderly and effective response to Blitzkrieg in the initial period of war – on maps – had little in common with the chaos, confusion and headlong Soviet retreat which followed the German invasion of June 22". (Roberts, 1995, p. 1313).

THE PRE-WAR OPERATIONAL WARGAMES OF THE SOVIET UNION

It should be noted that in February 1941 the Soviet Union was conducting the wargames not only on the western war theatre, but also in the south theatres and some other military districts. For instance, in February 1941, Senior Instructor of the 7th Department of the Main Directorate of Political Propaganda and Culture of the Red Army (GUppKA), I.P. Baikov, travelled to Tashkent to participate in a military-operational game of the Central Asian Military District (Невежин/Neveczhin, 1997, p. 124). In general, the Russian historians found the evidences from the Russian archives that only in the last six months before the actual start of the war were conducted the following wargames:

- Operational map exercise in the Baltic Military District (February);
- Bilateral encirclement operational exercise in the Odessa Military District (February);
- Field trip of staffs of the Leningrad, Ural, and Orel Military Districts (March);
- Field trip in the Arkhangelsk Military District (March);
- Operational military exercise in the Moscow Military District (March);
- Bilateral operational exercise in the Kharkov Military District (May);
- Frontline operational exercise in the Western Military District (March);
- Frontline field trip in the Baltic Military District (April);
- Staff operational-strategic exercise in the Arkhangelsk Military District (April);
- Command operational exercise in the Moscow Military District (May);
- Frontline operational exercise in the Kyiv Military District (May);

- Joint exercises of the staffs of the Transcaucasian Military District and the Caspian Military Flotilla (May);
- Frontline field trip in the Baltic Military District (June) (Солонин/Solonin).

The level and importance of these games was less than of those that were held in Moscow, but it is clear that thorough preparation for big war would require organization of multilevel exercises from strategic, operational to tactical. Eventually, all these levels should be integrated into one conceptual picture of war. Russian historian Mark Solonin exactly proves in his article that at the operational and front level the Soviets were preparing for the joint-offensive operation. He refers to the exercises that were organized in the Kyiv Military District (future South-Western front). According to the plan, the strongest concentration of forces had to be in this theatre. Moscow prepared attacks on the Lublin direction, together with Western front (Belarus). The General Staff had many other operative level games with the *"legend"* similar to two strategic games, but Solonin writes that if the strategic games were too ambitious, the operative level of the games as close as to the final date of 24 June 1941 became less ambitious and nobody even thought to attack Warsaw or Budapest.

MILITARY AND GEOPOLITICAL IMPLICATIONS TO THE COLD WAR

As it was indicated above, the Soviet military leadership did not have much experience in conducting massive military operations. They had the experience of the First World War, the Civil War, and Battles of Khalkhin Gol, and the war against Finland in 1940. Thus, at the end of 1940 and in January 1941, the Soviet command made the first big attempt to learn and accumulate the experiences and modern theories of warfare in several important wargames. In these games, the Soviet military command was learning how to fight big industrial wars and see the war as an integral part of the grand strategy. It was not a coincidence that immediately after the wargames the Soviet military command was seriously reshuffled and to power came younger and more advanced thinkers in terms of understanding the logic of future industrial wars. However, it should be noted that Zhukov confessed in his notes the following: *"It must be frankly said that neither the people's commissar nor I had the necessary experience in preparing the armed forces for such a war that unfolded in 1941, and, as you know, experienced military personnel were exterminated in 1937-1939".* (Документы: 1941 год: Кн. 1, Documents: Year 1941, p. 500).

The wargames and the future experience during the military campaigns against Germany once again strengthened the Soviet and Russian position regarding the concept of strategic depth and the western war theatre was going to be the central theatre in case of war with the West during the Cold War. If we speak about the 21st century, we again can see that Russia recalls its operational-strategic art on the doctrinal and practical levels.

CONCLUSIONS

In the two games the Blue attacked and the Red counterattacked. In both cases, the Soviet command pursued the goal to push the enemy out of the state borders and give the general battle on the territory of the enemy or at least finish with the remaining forces yet on the enemy's territory. In both cases, it was the territory of contemporary Poland, which was under the control of Germany. In both games, it was important to reach the Vistula River. Most of the participants, from the Red and the Blue sides, had to solve problems in games. The same goal was pursued by the Soviet Russian General Mikhail Tuchachevsky in 1920 regarding Warsaw.

In terms of getting senior officers to practice leading troops in operations, the games achieved their goal; at the same time, they showed that many top-level commanders did not yet possess the necessary operational-strategic outlook, the art of troop control in the dynamics of operations. In both games, the Red was able to push the Red forces out of Soviet territory. This part of the games has not been disclosed properly. The Soviet command did not seriously elaborate on that initial stage of the war and concentrated rather on the operations than on developing sufficient defence in case of a massive attack of the Blue, which prevented an easy counterattack in the initial stage of the war. In the games was made the most dramatic error, the Soviet Stavka expected the main strike in the Ukrainian direction and Kyiv. The commanders were running the units, operations, and areas they had not commanded in the real war. Many commanders were from different military districts that had not dealt with the Germans at the first stage of the war.

After 1945 the information about these wargames was sealed in the archives, but definitely some part of the Soviet General Staff Academy and part of the military leadership of the USSR knew about these wargames. The first hectic mentions of the game exactly came from different memoirs of Soviet generals and historians. However, exactly these games institutionalized and systematized the Soviet military thinking and became the first intellectual grounds for the future wargames during the Cold War.

The modern geopolitical and military situation, as well as the current circumstances, require the military command of the NATO countries to constantly conduct in-depth wargames with the involvement of political and military leadership. Warfare in the 21st century more than ever demands the participation of economic, political, and social leadership in the process of planning and development of war scenarios.

BIBLIOGRAPHY:

1. Белоусова, З.С./Belousov, Z.S. (1992). *„План Бриана и позиция СССР в свете новых документов”*. Новая и новейшая история, № 6.
2. Бобылев, П.Н./Bobylev, P.N. (1993). *„Репетиция Катастрофы: (По материалам совещания высшего командного состава Красной Армии в декабре 1940 г. и оперативно-стратегических игр на картах в январе 1941 г.)”*. Военно-Исторический Журнал, No. 7; 8.
3. Бобылёв, П.Н./Bobylev, P.N. (1995). *„К какой войне готовился Генеральный штаб РККА в 1941 году?”*. Отечественная история, No. 5, http://militera.org/research/articles/b/t41555/, retrieved on 12 May 2024.
4. Collection of Articles of the Journal *“Military Thought”*, No. 3(73)/1964 and No. 2/1965, https://www.cia.gov/readingroom/docs/CIA-RDP10-00105R000201700001-6.pdf, retrieved on 15 June 2024.
5. Гайворонский, К./Gayvoronsky, K. *„15 роковых дней. Главная загадка советского военного планирования 1941 года”*. История.ру, 13.02.2021, http://istorya.ru/forum/index.php?showtopic=9451, retrieved on 22 May 2024.
6. История военной стратегии России/History of Russian military strategy (2000). М.: Кучково поле; Полиграфресурсы.
7. 1941 год: В 2 кн. Кн.1/Сост. Л.Е.Решин и др.; Под ред. В.П.Наумова; Вступ. ст. акад. А.Н.Яковлева. – М.: Междунар. фонд «Демократия», 1998. – (Серия «Россия. XX век. Документы»).
8. Мельтюхов, М.И./Meltukhov, M.I. (2000). *Упущенный шанс Сталина. Советский Союз и борьба за Европу: 1939-1941*. – М.: Вече, http://militera.lib.ru/research/meltyukhov/10.html#, retrieved on 27 June 2024.
9. Военно-Исторический Журнал/Military-Historical Journal (1993), No. 6. БобылевП.Н. *„Репетиция Катастрофы: (По материалам совещания высшего командного состава Красной Армии в декабре 1940 г. и оперативно-стратегических игр на картах в январе 1941 г.)”*.
10. Parallel History Project/PHP, Publications Series (May 2000). *“Taking Lyon on the Ninth Day? The 1964 Warsaw Pact Plan for a Nuclear War in Europe and Related Documents”*. Washington, D.C./Zürich.
11. Roberts, C. (Dec., 1995). *Planning for War: The Red Army and the Catastrophe of 1941.* Europe-Asia Studies, Vol. 47, No. 8.

12. Русский архив/Russian Archive (1993). Великая Отечественная. Т. 12 (1-2). Накануне войны. Материалы совещания высшего руководящего состава РККА 23-31 декабря 1940 г. – М.: ТЕРРА, http://militera.lib.ru/docs/da/sov-new-1940/32.html#, retrieved on 22 May 2024.
13. Шерстнев, В./Sherstnev, V. (2005). *„Трагедия сорок первого. Документы и размышления”.* Смоленск. “Русич”.
14. Соколов, Б.В/Sokolov, B.V. (2000). *Неизвестный Жуков: портрет без ретуши в зеркале эпохи*. – Мн.: Родиола.
15. Солонин, М./Solonin, M. *„Игры 1941-го года”*. Военное Обозрение, 8 Декабря 2012//https://topwar.ru/21830-igry-41-go-goda.html, retrieved on 18 May 2024.
16. Захаров, М.В./Zakharov, M.V. (1989). *„Генеральный штаб в предвоенные годы”*, М.
17. Жуков, Г.К./Zhukov, G.K. (1986). *Воспоминания и размышления*. М., Т. 1.
18. Жуков, Г.К./Zhukov, G.K. (2002). *Воспоминания и размышления*. Т. 1. – М.: Олма-Пресс.

STRATEGIC COMMUNICATION – ESSENTIAL TOOL IN SUPPORT OF ROMANIA'S NATIONAL SECURITY IN THE CURRENT GEOPOLITICAL CONTEXT –

Colonel Daniel Ionel Andrei NISTOR
"Carol I" National Defence University, Bucharest
DOI: 10.55535/RMT.2024.4.28

Strategic communication plays an essential role for improving security culture. While the term has grown in popularity, its meaning often gets muddled as various forms of communication – whether organizational, public affairs, or crisis communication – are labelled as strategic. In Romania, strategic communication has evolved similarly to neighbouring countries, aligning with NATO and EU practices. However, the lack of a national framework has led to fragmented efforts, with no single institution coordinating these activities. The Ministry of Defence (MoD) has adapted NATO's Strategic Communication (StratCom) approach, integrating public relations, psychological operations (PSYOPS), and information operations (InfoOps) to enhance security on NATO's Eastern Flank. The Ministry of Foreign Affairs (MFA) uses StratCom to combat disinformation, following the EU model. Despite adopting a National StratCom strategy in 2021, Romania lacks a unified body to synchronize communication at the national level, hindering support for national objectives. This paper proposes an empirical analysis of the author to improve institutional strategic communication to strengthen Romania's security culture, offering recommendations for improvement.

Keywords: strategic communication; security culture; influence; framework; strategy;

INTRODUCTION

For some time now, we have been witnessing a reconfiguration of relations between the main strategic actors, which has resulted in a new security paradigm with elements of instability in almost every geographical area, including Russia's aggression against Ukraine in Europe, conflicts on the African continent, a tense relationship between China and Taiwan, the conflict in the Gaza Strip, tensions between India and Pakistan, and conflict between Armenia and Azerbaijan. These are just a few examples of the 59 wars and armed conflicts documented in the world in 2023 alone, a record of interstate conflicts following the Second World War with over 120,000 casualties (Rustad, 2024, pp. 7-8, HIK, 2023). When we combine all of the mentioned aspects with the factors unique to economic, energy, and diplomatic issues, we get a clear image not only of strategic actor rivalry, but also of the security situation's volatility, unpredictability, and decreasing predictability. When discussing security or relations between states or organizations, whether economic or political-military, it is critical to understand the context as well as the level of willingness and ability to communicate and position themselves at the diplomatic, strategic, and organizational levels.

We can discuss decisions and actions at the international relations system level, as well as the impact and reconfiguration of the relationship system, but we can only understand it to a limited extent if we do not also observe the communication and positioning side, the way actors communicate strategically at the national, regional, or international level, even when they do not communicate (strategic silence). Whether we are discussing cooperative or conflictive relations between states or between states and organizations, strategic communication is the connecting element, because we are not only talking about strategic discussions, but also about the alignment of facts with words, the synchronization of actions, and the creation of strategic effects, including the use of strategic ambiguity.

We will examine the concept of strategic communication by reviewing over 20 official and scholarly definitions and interpretations, as well as presenting NATO and EU approaches to which we will report the institutional strategic communication in Romania. Based on our own analysis and experience, we will make a number of observations to improve the process.

Institutional strategic communication must also be understood, adapted, and integrated into the national security paradigm in order to achieve institutional coherence, on the one hand, and population information and support, on the other hand, to support the country's national, European, and Euro-Atlantic approaches. It is critical to understand not just the role of strategic communication in security, but also its impact on the interplay of domains ranging from military to economic, socio-political, and cultural, because the majority of the impact factors are found in the multi-domain approach.

WHAT IS STRATEGIC COMMUNICATION?

Strategic communication has become a very popular term in recent years, loaded with a mixture of enthusiasm and confusion, because any type of communication has become *"strategic"*, whether it should be called organizational, institutional, or internal, or public affairs, public relations, public diplomacy, or crisis communication, using a field classification, and the confusion expands as functions are frequently combined with processes, actions, or domains. Strategic communication is characterized differently at the institutional level: as a function, process, mentality, or a mix of all three. And, in terms of semantics, the understanding of the concept varies from similar to wholly different depending on the expert, organization or institution.

Communication and Strategy – Two Terms and More Concepts

The combining of two terms created a new concept: strategic communication. Analysing semantically, we could understand that the concept suggests, firstly, that the activities are strategic, with strategic, planned, and intentional objectives, and secondly, that the communication should be for the fulfilment of the objectives of the institution or organization; normally, the concept of strategy should not be defined in a restrictive way, as it has expanded and been incorporated into many fields, from military art to the area of marketing (Wilson et al., 2019, p. 144).

The concept of strategic communication was used in the early 1950s with *"reference to competitive organizations on the labour market in their endeavour to obtain advantageous market shares"* (Popescu, 2022, p. 51), but for a long time it was used as a synonym for the term public relations, being mainly used to define political persuasion, promote advocacy and litigation, crisis communication, communication, and brand-building services (Hallahan et al., 2007, p. 12). In the 1940s and 1950s, public relations advice shifted to controlling an organization's reputation, aligning campaigns with goals and strategy (Trevena, 2023).

Moss and Warnaby (1998, p. 135) attempt to clarify the terms: communication strategy refers to the manner in which an organization communicates the strategic vision of its stakeholders, as well as the plan by which the organization implements the strategy (*communication strategy*), whereas *strategic communication* refers to communication that is *planned and executed strategically*, and the translation of the terms (in Romanian) does not appear to reduce confusion. And, as Löffelholz (et al., 2017, p. 441) notes, with a few minor exceptions, such as Hallahan or Holtzhausen, the majority of the authors emphasize the concept of *"communication"* rather than *"strategy"*, the latter being more linked with the discipline of management.

Following the 11 September 2001 terrorist attacks, three elements of communication emerged inside the George W. Bush Administration in the United States: (a) information and psychological operations, (b) public affairs, and (c) defence assistance for public diplomacy. It was accomplished by dedicating integrated communication technology to the pursuit of tactics, operations, and other specific elements of national strategy in this so-called *"war of perceptions"*, with the goal of winning credibility and hence freedom of action. At the time, many people involved in national security and defence matters began to use the term *"strategic communication"* (Paul, 2011, p. 27).

Hallahan (2007) examines the concept of strategic communication through the lens of two distinct concepts – strategy and communication – and argues that the strategic nature of the activities ensures that they *"are neither random nor unintentional"*, even if the achievement of an organization's strategic objectives can be hampered by the negative impact resulting from the unintended consequences of the organization's or third parties' communication. The author adds that the term *"strategic"* should not be strictly defined, but rather broadly explored and understood as a multidimensional notion, and that strategic communication must see communication as a *"constitutive activity of management"* (Hallahan et al., 2007, p. 27).

Common Elements and Differences in Understanding and Defining the Concept

We have examined more than 20 definitions of strategic communication at the organizational, institutional and academic levels, and, despite variations in definitions, there are several similarities and differences across sources, particularly in terms of purpose, process and applicability in civilian, military and government contexts. As Paul (2007) observed, *"despite the lack of an agreed definition, there's a vague sense of consensus that when one of us says strategic communication,*

we all know what we're talking about". Strategic communication (StratCom) is a sophisticated concept that focuses on influencing the audience and attaining particular goals through coordinated messages and actions.

Common Elements of the Definitions of Strategic Communication Concept (StratCom)

Several definitions consider strategic communication as a process rather than a collection of actions. According to the United States Department of Defense (2009, p. 3) and Christopher Paul (2011, p. 190), public perception is factored into policymaking and operations, coordinated activities, messages, and visuals are essential for influencing audiences. According to Murphy (2009, p. 9), effective StratCom entails arranging actions and messages to produce cognitive consequences, which necessitates continual synchronization across all levels. Another common aspect is the incorporation of several communication methods.

Strategic communication is defined by the White House (2010, p. 2) as the coordinated use of words and deeds in public diplomacy, public affairs, and information operations. According to Goldman (2007, p. 3), effective communication requires the alignment of numerous factors with national objectives. NATO Communication (MC-628, 2017, p. 9) broadens the integration of psychological and information operations to influence the information environment, echoing Murphy's (2009, p. 9) focus on the military's role in coordinated communications.

Most definitions highlight the significance of audience participation and perception. The White House (Ib.) highlights that strategic communication is concerned with how communication is received by the intended audience. Murphy (Ib.) and Paul (2008, p. 7) emphasize the cognitive importance of strategic communication. According to Guererro-Castro (2012, p. 7), in a security environment, effective StratCom must combat conflicting wills in international scenarios such as crises or wars while remaining aligned with national interests.

Finally, it is typical to see communication initiatives aligned with national or company goals. Murphy (Ib.) and Paul (2011, p. 190) emphasize the promotion of national interests, but Goldman (2007, p. 3) regards StratCom as a tool for influencing behaviours to achieve national goals. Argenti, Howell, and Beck (2005) argue that aligning communication with organizational strategy enhances strategic positioning (Wakefield et al., 2015, p. 353).

Elements of Differentiation of the Concept of Strategic Communication (StratCom)

While there are some parallels, definitions of strategic communication differ greatly, especially in terms of scope and context. Military-oriented definitions, such as those provided by the United States Department of Defense (DOD, 2009, p. 1), Murphy (Ib.), and NATO (MC-628, 2017, p. 9), stress the role of StratCom in national defence and military operations, with a focus on synchronized communications to support security goals.

Civil, corporate-oriented definitions, such as those of Argenti, Howell, and Beck (2005), Hallahan (2007) and Werder (2018), regard strategic communication as a tool for increasing a company's competitiveness. StratCom is commonly viewed as an instrument for wielding power and influence (Wakefield et al., ib.). Goldman (Ib.) sees it as a weapon for influencing attitudes and actions, emphasizing its potential as a tool of national power. Grunig (2011, p. 13) observes, on a more critical note, that many practitioners still regard communication as a tactical activity rather than a strategic management role, indicating a tension between communication as a tool of influence and as a broader organizational function. There are several techniques of timing words and actions. The White House (Ib., p. 3) and Gramaglia (2008, p. 10) emphasize the importance of timing actions and messages to encourage consistent communication and behaviour. Guererro-Castro (2012) focuses on the concept of *"logic of action"* in scenarios such as war and crisis, emphasizing the need for strategic communication in high-stakes situations.

Finally, the emphasis on cognitive impact differs from publication to publication. Murphy (2009) and Paul (2011, p. 119) investigate the impact of strategic messaging on public perception, whereas Hallahan et al. (2007) consider it as a mission-oriented goal that transcends military or government contexts. According to the UK Ministry of Defence (2023), even inaction can influence perceptions, emphasizing the complexities of public reception (AJP-10, UK, 2023, p. 25).

In conclusion, strategic communication is defined as a process that integrates coordinated communication operations to achieve national, organizational, or security goals. While military definitions highlight the synchronization of words and actions to help combat operations, civilian and institutional perspectives focus on broader strategic alignment and public impact. These definitions all agree that effective strategic communication is dependent on the combination of several communication capabilities, the recognition of public perceptions and the support of large objectives, and that the context, whether military, political, or corporate, determines the specific focus and application of strategic communication elements.

Although the definitions have changed throughout time to provide clarity to the process, some of the parts have remained applicable. Strategic communication is goal-oriented, requires coordination and synchronization of words with actions, of what you do with what you say, and involves a target audience, as well as a message specifically designed to influence the audience. It is both a process and a paradigm that recognizes that information and perception have an effect on the target audience's behaviour and that the activity must be calibrated in relation to the effects.

Strategic Communication Domains

Reflecting the classification of communication practices in academia, Hallahan (2004) presents four of the areas from which strategic communication can be drawn: (a) corporate communication; (b) marketing, advertising, and public relations; (c) business communication; and (d) academic studies of organizational behaviour in general (Hallahan, 2004, p. 162). Popescu (2022, p. 87) takes up Haiden's (2017) idea of a transdisciplinary model that relates the capabilities of strategic communication in relation to their area of action. The political area includes actions in the direction of public affairs, public relations, public diplomacy and *soft power*, while the military area includes actions in the direction of psychological operations, information operations and *hard power*, and the commercial area involves actions in the direction of branding and marketing, while, classified by sphere of interest and applicability, strategic communication *"converges towards a trans-disciplinarity, with notions related to marketing, sociology, communication psychology, semantics, cultural studies, administrative policy, and public relations"* (Popescu, 2022, p. 58).

Some authors consider public diplomacy and strategic communication to be synonymous, encompassing activities in which governments and groups interact with mediated attitudes, cultures, and environments, advise on policies, and affect behaviour (Gregory, 2005). These researchers have a broad vision of strategic communication. However, other authors do not make obvious differences between the two concepts (e.g., Deutsch, 2010; Hayden, 2010), while others, such as Nye (2004), consider strategic communication to be a subset of public diplomacy. According to Leonard (et al., 2002, p. 11), it is one of the three pillars of public diplomacy that deals primarily with proactively creating news agendas and influencing opinions. In contrast, many military-political researchers, including those from the Department of Defense (2004), Goldman (2007), Murphy (2008) and Paul (2011), see strategic communication as the overarching concept, integrating public diplomacy, public affairs, and military psychological operations to coordinate messages (Löffelholz, et al., 2015, p. 441), and Paul (2010, p. 11) emphasizes

that *"the elements of transmission, dissemination and engagement specific to strategic communication are communication, information and influence capabilities"*.

In an attempt to define the areas of responsibility of strategic communication and, at the same time, to comply with the national and Euro-Atlantic framework, the National Strategy for Strategic Communication and Combating Disinformation/ NSSCCD (2021) takes up the dimensions of the National Strategy for the Defence of the Country 2020-2024 and introduces them as areas: diplomatic dimension; defence; public order; intelligence, counterintelligence and security; economic and energy; crisis management and civil protection; environmental security, with direct effects in terms of ensuring the quality of life; education, health, social and demographic (NSSCCD, 2021, p. 6).

Strategic Communication – a Tool for Information or Influence?

Even while the term influence appears to have a bad meaning in popular culture, since it is commonly connected with manipulation, it should be highlighted that the communication process itself is a form of influence. We do not communicate just to communicate; we communicate to impart information, a message, and we expect it to have an impact, whether it is a reaction, increased awareness, or a change in conduct. To effectively deliver the message, we must realize that our information/ communication is a process of influence. It applies not only to marketing, which has the mission of executing influencer messages to change an audience's behaviour from neutral to buyer or supporter of a product or brand, but also to public, institutional communication, which has the role of educating and informing. The message's success is determined by the production of the influence effect, which results in a reaction, whether it is acceptance, non-acceptance, or a change in the recipient's attitudes, behaviours, or values. Most differences about influencing vs. informing occur when we discuss the aim of the intention to influence, which appears to lean more toward manipulating.

Goldman, a strategic communication adviser in the Bush administration, described strategic communications as *"a powerful tool to support national goals, a means of influencing attitudes and behaviour, a process of listening to and engaging the public, and coordinating messaging within government and with allies",* emphasizing that it "*means both words and deeds"* (Goldman, 2007, p. 6), but also mentioning the warning that simply speaking or acting without communicating can undermine the impact and credibility of actions.

At the same time, Hallahan (2015, p. 244) emphasizes that when *"viewed from a modernist perspective, the results, strategically pursued, smell of control*

and manipulation" and shows that the central element of strategic communication is the idea of influence, invoking, on the one hand, *"the ability to cause effects, and, on the other hand, the tools available for behaviour change, from physical force to persuasion, the latter requiring communication to create the idea of acceptance"* (Hallahan et al., 2007, p. 24). In terms of information accumulation and influencing effects, communication becomes strategic when it is subordinated to the achievement of political-military goals, when it is planned, coordinated, and applied synchronously in support of the achievement of strategic, political and military, national and allied, objectives (Vasile, 2017, p. 48).

The UK Government Communication Group adds influence to the concept of strategic communication by emphasizing the need to *"influence the public for the public good by mobilizing the resources necessary to achieve agreed-upon objectives"* (UK GCS, 2021, p. 3). The level of participation in the planning and management processes impacts the efficacy of strategic communication. Paul (2009) emphasizes the importance of institutional commitment and leadership involvement in enterprise-level strategic communication activities, arguing that the decision-making process must consider the impact of international public opinion on policy and vice versa (Paul, p. 13).

STRATEGIC COMMUNICATION AT NATO AND EUROPEAN UNION LEVEL

Strategic communication plays a key role within NATO and the European Union, with the aim of supporting security objectives by delivering clear, coherent, and tailored messages to different audiences. In a global context where instability and disinformation are increasingly present, the ability to communicate effectively and strategically is vital to protect democratic values, promote international cooperation, and maintain public trust. NATO and the European Union are coordinating their efforts to counter negative influence campaigns and build global information resilience in an attempt to demonstrate that well-structured communication is an important pillar for regional and global security and stability.

Strategic Communication at NATO Level

The communication process within the North Atlantic Alliance is complicated by the alliance's very complexity: 32 independent, sovereign states, geographically arranged on several continents, with different socio-political-military organizations, which must communicate in an integrated manner decisions unanimously accepted at the alliance and state levels, connected to the principles of transparency and credibility.

Strategic communication has proven to be the appropriate solution to the requirement for institutional communication synchronization, both at the internal level (from political to political-military and military) and at the state level (political and military). The process of definition and implementation was difficult, and the regulatory attempt has undergone transformations and adaptations since 2009, from the approval of the first strategic communication policy through the adoption and establishment of the concept in 2017 to the development of a specialized manual and a strategic communication doctrine (AJP-10). NATO's Public Diplomacy structure stated in 2009 that *"comprehending the benefits and complexities of StratCom takes time and education"*, both inside the Alliance and for the general public (NATO DSG-0528, 2010).

In the context of NATO, strategic communication entails *"the coordinated and appropriate use of NATO's communication activities and capabilities – public diplomacy, public relations, military public relations, information operations, and psychological operations, as appropriate – in support of the Alliance's policies, operations, and actions"* (SG-0794, 2009). Strategic communication or StratCom *"in the NATO context, represents the integration of communication capabilities and the information function with other military activities in order to understand and shape the information environment in support of NATO goals and objectives"* (MC-0628, 2017, p. 3). NATO's Strategic Communication is a leadership characteristic that focuses on improving the Alliance's ability to clearly explain its narratives, themes, and messages to external and internal audiences. NATO StratCom provides strategic political and military counsel and direction based on the North Atlantic Council's approved information strategy.

Propaganda actions can have a negative impact on the public's attitudes and behaviours, and StratCom can be used not only to combat propaganda, but also as part of NATO's effort to properly inform and influence the audience through actions and words in order to shape the security environment and ensure timely and coherent information-based action. StratCom exists to synchronize the message at all levels in order to maintain credibility and reduce the gap between *"saying and doing"* by using clear and simple messages that are coordinated and fully integrated at all levels, from political to strategic, operational, and tactical ones. Strategic communication is *"about creating effects in the information environment"*, and the tactics used to do it include public diplomacy, military public relations, psychology, and information operations. Psychological and information operations are military-specific instruments that improve strategic communication while preserving their functional role in military operations (MC-0628, 2017, p. 4).

Furthermore, by adopting the NATO Strategic Concept (2022), the Alliance commits to ensuring greater integration and coherence of capabilities and activities across all areas and spectrums of conflict, emphasizing that it *"will continue to maintain credible deterrence, strengthen strategic communication, increase the effectiveness of exercises, and reduce strategic risks"* (NATO, 2022, p. 3).

As a natural adaptation to the new security challenges, for the synchronization and efficiency of communication, the AJP-10 Strategic Communication Doctrine was adopted at NATO level in 2023 and provides guidance to NATO commanders and personnel at all levels and supports the goals and objectives of the Alliance by understanding and shaping the information environment and details, at the military level, the relationship of StratCom with the integration function (information operations) and communication and influence (relations, public, military, and psychological operations) (AJP-10, 2023, p. xvii). A natural setting of the communication process is the doctrinal framework, with emphasis on the connection between the audience, the information environment, and the effects generated in the cognitive field, beyond the virtual (cyber) or physical (terrestrial, air, sea, space) domain.

All of these instruments have been designed and developed to help the Alliance achieve its objectives and goals by establishing a doctrinal and legislative framework at the alliance level, increasing interoperability, standardizing procedures for joint operations and activities, as well as setting the framework for simplifying the implementation of the strategic communication process at the national level, making it easy to transform and implement.

The European Union and Strategic Communication

After Russia's illegal annexation of the Crimean Peninsula, in 2014, the European Union began to address the issue of disinformation, and, in 2015, it created a joint capacity to counter propaganda, stressing the need to counter Russia's disinformation campaigns. The European Council defined strategic communication as an *"important tool in promoting the EU's overall policy objectives"* and created the EastStratCom communication team within the European External Action Service (Action Plan on Strategic Communication, 2015). In the context of migration and radicalization, another working group, StratCom, was formed to promote dialogue between Arab and European communities through public diplomacy (EUISS Report, 2016).

The 2015 EU Action Plan stresses the importance of effective communication to promote EU policies and values, supporting media independence, and improving the capacity to respond to disinformation (Action Plan on Strategic Communication,

2015). In 2016, the EU established the Common Framework for Countering Hybrid Action, which included awareness-raising, crisis prevention, and response measures, cooperating closely with NATO (Common EU Framework, 2016). The 2016 NATO-EU Joint Declaration, renewed at the Brussels (2023) and Washington (2024) summits, reinforced these actions on resilience and information sharing (Joint Declaration, 2023).

The EU Global Strategy (2019) focuses on combatting fake news and promoting Union values through timely and effective strategic communication (EEAS, 2021). It involves promoting press freedom and media pluralism in the eastern territories, particularly Ukraine, Moldova, and Georgia, using resources available in Russian (EU Joint Communication, 2019).

Strategic communication is an important instrument for the EU, and it is also included into the European Union's Global Strategy (EEAS, 2016), a strategy that has been constantly analysed and refined. In a review of the 2019 strategy's implementation and the need for an update, the EU prioritizes public diplomacy and strategic communication to combat disinformation and boost responsiveness and visibility. The European External Action Service has established three Task Forces for Strategic Communication, highlighting the importance of this sector in policy. The EU intends to increase its efforts by combating disinformation and effectively conveying its objectives to global partners and European citizens.

At the same time, the EU places a high value on strategic communication to improve its credibility, responsiveness, and coherence in implementing its aims. Credibility, a critical issue, is created by constant political will and a collaborative ability to carry out agreed-upon policies, supported by substantial financial investment. The planned €30 billion increase in the Multiannual Financial Framework (MFF) for foreign and defence policy demonstrates the EU's commitment to global responsibilities. Furthermore, initiatives such as the establishment of the Neighbourhood, Development, and International Cooperation Instrument (NDICI) reflect the EU's desire to act independently in areas such as development and humanitarian aid (EUGS, 2019, p. 12).

ROMANIA AND INSTITUTIONAL STRATEGIC COMMUNICATION – A STRATEGY AND SEVERAL PLANS

At the institutional level, strategic communication in Romania has followed a path of sectoral mirroring, or imitation, of the processes and functions of the North Atlantic Treaty Organization (MoND) and the European Union (MFA). Until 2021, Romania lacked a national strategic communication strategy, instead relying on sectoral elements at the relevant ministries that were incorporated into planning

papers based on choices and directives agreed upon by the two institutions. If NATO adopted the MC-0628 directive on strategic communication in 2017, response elements were established at the national level by the Ministries of National Defence, Foreign Affairs, and Internal Affairs, as well as concepts for strategic communication organization and processes, functions, or capabilities. The other institutions lack the components required to integrate and enable institutional strategic communication. There is no organization inside the President's or Government's institutions that is responsible for strategic communication, strategy implementation (NSSCCD, 2021), or national strategic communication synchronization.

The National Strategy for Strategic Communication and Combating Disinformation (2021), adopted by the Supreme Council for the Defence of the Country Resolution no. 113/2021, derived from the National Strategy for the Defence of the Country 2020-2024 (NSDC) and the European Union Action Plan against Disinformation, aims to *"increase the resilience of society, media literacy and the reaction capacity of the authorities"*, and defines institutional strategic communication as *"the set of actions planned and carried out in a coordinated manner, in the field of communication, materialized in the public discourse, in order to promote Romania's national interests"* (NSSCCD, 2021). At the level of the Executive, in the Government Communication Management Strategy (GCMS, 2023, p. 2), strategic communication is defined as *"a component of strategic management within the government, which refers to a consistent, long-term dialogue between it and the various stakeholders. Communication is strategic when it is aligned with the organization's mission and vision, contributing to their achievement"* (Ib.), a definition that we could say is very close to that of organizational communication, with a preponderant emphasis on the unilateral/unidirectional nature of communication.

As for the NSSCCD definition, we could consider it vague and limiting by using the formulation *"in the sphere of communication"*, because the phenomenon of disinformation also unfolds beyond the sphere of communication, and *"materialization in public discourse"* suggests a reactive strategy, a defensive response to what is already present in public discourse, without using the function of prevention and early warning. Similarly, *"the promotion of Romania's national interests"* can potentially create a stance that contradicts the state-citizen relationship, as the state's interests may not always align with the well-being of its citizens.

The fight against disinformation aims to enhance societal resilience while also generating adapted response options and crisis situations. The key element in this effort is inter-institutional cooperation, which is achieved through a system based on prevention and education policies, practices, and activities, risk assessments, and early warning. These elements enhance the institutional capacity to respond swiftly

to a crisis or a disinformation campaign that may trigger a crisis. The strategy's areas of activity align with those outlined in the National Strategy for the Defence of the Country 2020-2024, encompassing defence and public order, economic and energy, crisis management, civil protection, and educational, health, social, and demographic aspects.

The National Strategy for Strategic Communication and Combating Disinformation (2021) aims to create a unitary communication identity for the Romanian state, improve the communication capacity of the authorities, increase media literacy and strategic culture, and strengthen society's resilience. It also promotes critical thinking, fact-checking, and disinformation detection mechanisms, involving the media, civil society, and academia, and the intensification of cooperation with European and Euro-Atlantic partners (NSSCCD, 2021).

This approach aims to emphasize the inseparable nature of two key components: strategic communication and combating disinformation. Conceptually analysing the statement, we **disagree with the strategy (NSSCCD)**, viewing disinformation as a process that is subsumed under communication, originating from either defective communication or a lack of exercise in communication. At the same time, the phenomenon of disinformation is present in the public space, but the means of production and propagation are not all associated with the phenomenon of strategic communication; the manifestation in the cyber field can be an example in this regard. We must view disinformation as a phenomenon or process that can emerge and impact various fields, with the audience's influence serving as the defining element.

Strategic communication is an effective tool in support of Romania's national security in the current geopolitical context to the extent that it manages to calibrate the communication elements to the specificity of the audience, and to integrate and apply the elements of the communication strategy/NSSCCD that aim to *"increase societal resilience in the face of threats in the public communication space, the degree of media literacy, and the development of the response capabilities of the Romanian public authorities"* (NSSCCD, 2021, p. 1). These objectives are intended to meet the requirements of the NSDC (2020-2024, p. 9) to ensure the *"security of the citizen and the nation in the national and international framework"* as well as those of the European Union's Action Plan against Disinformation (2016).

Strategic communication achieves both horizontal synchronization and coordination of information and public relations structures representative of the fields of activity (as specified in the document), as well as the transmission of a unitary and coherent message to internal and external stakeholders.

INSTEAD OF CONCLUSIONS. WHY IS STRATEGIC COMMUNICATION DIFFERENT IN ROMANIA, AND HOW CAN IT BE MORE EFFECTIVE?

Romania has a strategic communication strategy at the national level as well as structures within a few ministries and other governmental institutions, processes or functions, but there is no structure that synchronizes institutional communication and alignment at the national level with international structures or organizations in order to achieve national strategic goals.

Strategic communication is about professionals, dedicated people who understand the process, but it is also about high-level leadership and institutional ownership, as well as the synchronization of the messages at the national and European and Euro-Atlantic levels. And then, at the national and institutional levels, we must grasp and assume the entire process, synchronize communication at the level of strategies and doctrines, and develop action plans and processes. Finally, education is required.

And, although today in everyday language any action, any process has become *"strategic"*, just as any communication has become *"strategic"*, we do not find a unitary understanding of the use of the term even at the institutional level, and although we have a working definition in the strategy, we remain tributary to the sectoral understanding of the term, by using it in the sense of communication at the strategic level, communication based on a strategy, or in another associated sense based on personal experience.

Strategic communication takes a holistic, comprehensive approach, understanding it as having a multiple nature, being both function and process, but also mindset, comprehensive toward the classic elements of communication – public relations, public affairs, institutional communication, interaction with the media – because, in addition to the classic processes of education and information, it also has the function of influencing and changing perceptions, attitudes, and mentality. So, the influencing process is the means by which it can be accomplished by appealing to the unique norms, values, and attitudes that contribute to the development of the security culture, and strategic communication brings together the relevant procedures and tools.

Increasing public awareness of the influence of disinformation campaigns can be done effectively through a mechanism of institutional collaboration and coordination, designed to work in the long term, with an open projection on civil society, with the involvement of civil society, the media and academia. NGOs and the private sector are a key element of the transition from the whole of government to the whole of society, but the process is somewhat difficult due to the low trust

of the citizen in the state institutions (Government – 19%, Presidency – 29%), and in the political class (Parliament – 17%), the degree of institutional corruption and bureaucracy (INSCOP, 2023). At the same time, the initiation of a national, strategic project in the field of education, with a focus on the issue of media literacy for the development of data and information verification reflexes, we could appreciate that it is not only necessary, but also urgent, because the battle for citizen protection has moved to the cognitive field for some time.

The implementation of strategic communication at the national level must include, in addition to *traditional* communication (media relations, post-activity press releases etc.) and *new media* (web, social networks etc.), an assumption on the part of the political factor and the direct involvement of the *institutional leadership*. It is also necessary to decentralize and orient the decision-making process on several levels of expertise and leadership, depending on the importance and relevance of the subject in question. The effectiveness of institutional strategic communication is given by synchronization at the institutional level and interinstitutional cooperation. At the level of the executive, strategic communication must be assumed; the National Strategy for Strategic Communication and Combating Disinformation (2021) must be transposed into a coherent plan with concrete measures, responsibilities, and tasks that lead to *"align words with deeds"*, to carry out actions and activities for the benefit of the citizen.

BIBLIOGRAPHY:

1. ACO AD 95 – 2 (2022), *Allied Command Directive Stategic Comunication.*
2. Presidential Administration (2020). *Strategia Națională de Apărare a Țării 2020-2024/ National Strategy for the Defence of the Country*. București
3. Conflict Barometer (2023). Heidelberg Institute (HIIK), https://hiik.de/conflict-barometer/current-version/?lang=en, retrieved on 9 September 2023.
4. European Commission (2016). *Framework on Countering Hybrid Threats. A European Union Response*. Brussels
5. European Commission (CE) (2021). *General Report on the EU Activities in 2021*, https://op.europa.eu/webpub/com/general-report-2021/ro/, retrieved on 2 September 2024.
6. Department of Defense (2009), *Report on Strategic Communication,* Washington, D.C., p. 1.
7. EUGS (2019). *The European Union Global Strategy three years on, looking forward*, https://www.eeas.europa.eu/sites/default/files/eu_global_strategy_2019.pdf, p. 12.
8. European Commission (2015). *Action Plan on Strategic Communication*. Brussels.
9. European Union Institute for Security Studies/EUISS (2016). *Report of the European Union Institute for Security Studies.*

10. European External Action Service/EEAS (2016). *Strategia globală de politică externă şi de securitate a Uniunii Europene*. Bruxelle Brussels, https://europa.eu/globalstrategy/sites/globalstrategy/files/eugs_ro_version.pdf, retrieved on 22 July 2024.
11. European External Action Service (EEAS) (2019). *De la viziune la acțiune: Strategia globală a UE în practică – după trei ani de la elaborare, privind către viitor*, https://www.eeas.europa.eu/eeas/de-la-viziune-la-acțiune-strategia-globală-ue-în-practică-după-trei-ani-de-la-elaborare_ro, retrieved on 5 September 2024.
12. Goldman, E. (6 October 2007). *Strategic Communication: A Tool for Asymmetric Warfare*. In *Small Wars Journal,* pp. 5-7
13. Gramaglia, C.S. (2008). *Strategic Communication: Distortion and White Noise*. In *Joint Information Operations Warfare Command*, *IO Sphere*, p. 10.
14. Gregory, B. (2005). *Public Diplomacy and Strategic Communication: Cultures, Firewalls, and Imported Norms.* American Political Science Association conference on international communication and conflict, http://www8.georgetown.edu/cct/apsa/papers/gregory.pdf, retrieved on 2 September 2024.
15. Guerrero-Castro, C. (2012). *Strategic Communication for Security & National Defense: Proposal for an Interdisciplinary Approach*. In The Quarterly Journal, pp. 27-52.
16. Romanian Government (2023). *Strategia de management al comunicării guvernamentale/Government Communication Management Strategy* (GCMS, 2023), SIPOCA 754, https://sgg.gov.ro/1/wp-content/uploads/2024/01/Strategie-de-comunicare-754.pdf, retrieved on 26 August 2024.
17. Hallahan, K. (2004). *Communication management. Encyclopaedia of Public Relationship*, vol. 1, Thousand Oaks, Sage, pp. 161-164.
18. Hallahan, K., Holtzhausen, D., Ruler, B., Verčič, D., Sriramesh, K. (2007). *Defining Strategic Communication*, in *International Journal of Strategic Communication,* DOI: 10.1080/15531180701285244, https://www.researchgate.net/publication/241730557, pp. 3-35.
19. Hallahan, K. (2015*). Organizational Goals and Communication Objectives in Strategic Communication*. The Routledge Handbook of Strategic Communication, Taylor and Francis, p. 244.
20. INSCOP (2023). *Sondaj de opinie național – octombrie-noiembrie 2023. Partea a V-a, Incredere institutți. După 10 ani: Comparație 2013-2023*, https://www.inscop.ro/wp-content/uploads/2023/11/14.11.2023-INSCOP-News.ro-Incredere-institutii.pdf, retrieved on 12 June 2024.
21. Heidelberg Institute for International Conflicts Research (HIIK), Conflict Barometer (HIIK) (2023), https://hiik.de/conflict-barometer/current-version/?lang=en, retrieved on 9 September 2023.
22. Leonard, M., Stead, C., Smewing, C. (2002). *Public diplomacy*. The Foreign Policy Centre.
23. Löffelholz, M., Auer, C., Srugies, A. (2015). *Strategic Dimensions of Public Diplomacy*. The Routledge Handbook of Strategic Communication, Taylor&Francis.
24. Moss, D., Warnaby, G. (1998). *Communications Strategy? Strategy Communication? Integrating different perspectives*. In *Journal of Marketing Communications,* 4 (3), pp. 131-140.
25. Murphy, D.M. (2009). *Strategic Communication, Information Operations Primer*, p. 9.
26. NATO AJP10 (2023). *Allied Joint Doctrine for Strategic Communication AJP-10*, Edition A, Version 1, Allied Joint Publication NSO.

27. NATO DSG 0528 (2010). *Military Concept for NATO Strategic Communication*.
28. NATO MC 628 (2017). *NATO Military Policy on Strategic Communications*. Brussels.
29. *NATO Strategic Communication Handbook* (2017). Brussels.
30. NATO (2022). *NATO Strategic Concept 2022*, www.nato.int, retrieved on 9 September 2022.
31. Nye, J.S. (2004). *Soft power. The means to success in world politics,* Public Affairs.
32. Paul, C. (2007). *Strategic Communication' is Vague*, 15 February 2023, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-56/jfq-56_10-13_Paul.pdf?ver=bqn9c1gLmMM_MqRVikeO2Q%3D%3D, retrieved on 21 July 2024.
33. Paul, C. (2008). *Information Operations: Doctrine and Practice: A Reference Handbook.* Westport, Conn.: Greenwood Publishing Group, 2008, p. 7.
34. Paul, C. (2009). *Whither Strategic Communication? A Survey of Current Proposals and Recommendations*, RAND Corporation Report, pp. 1-16.
35. Paul C. (2010). *"Strategic Communication" Is Vague Say What You Mean, Joint Force Quarterly*, no. 56, 1st quarter, p. 11.
36. Paul, C. (2011). *Strategic Communication – Origins, Concepts, and Current Debates*. Greenwood Publishing Group
37. Popescu M. (2022). *Comunicarea strategică a informației*. Craiova: Ed. Top Form.
38. Rowland, L., Tatham, S. (2010). *Strategic Communication & Influence Operations: Do We Really Get 'It'?* In Small Wars Journal, p. 7.
39. SG-0794 (2009). *NATO Strategic Communications Policy*.
40. SHAPE/ACO (2017). *Strategic Communications Framework.*
41. Strategia Națională de Comunicare Strategică și Combatere a Dezinformării/National Strategy for Strategic Communication and Combating Disinformation (NSSCCD), (2021). București, adopted by NSDC Resolution no. 113 on 18.08.2021.
42. Trevena, C. (2023). *The evolution of PR*, https://hatch.group/the-evolution-of-pr/, retrieved on 25 May 2023.
43. The White House (2010). *National Framework for Strategic Communication*, Washington, D.C.
44. U.S. Department of Defense (2004*). Report of the Defense Science Board Task Force on Strategic Communication*. Washington, D.C.: U.S. Department of Defense, https://irp.fas.org/agency/dod/dsb/commu, retrieved on 12 October 2024.
45. U.S. Department_of_Defense (2006). *Quadrennial Defense Review-Execution Roadmap for Strategic Communication,* www.dtic.mil/dtic/tr/fulltext/u2/a495367.pdf, retrieved on 17 February 2024.
46. U.S. Departament of Defense (2017). *Department of Defense Dictionary of Military and Associated Terms*, Washington.
47. U.S. Joint Forces Command, Commander's Handbook for Strategic Communication and Communication Strategy, Suffolk, Va.: U.S. Joint Forces Command Joint Warfighting Center, Version 3.0, 24 June 2010, p. xii.
48. Vasile, V. (2017). *Comunicarea strategică – repere conceptuale și evolutive* – (I), in *Gândirea militară românească*, pp. 47-60.
49. Wilson, L.J., Ogden, J.D., Wilson, C.E. (2019). *Strategic communication for social media and marketing*, ed. a 7-a, Kendal Hunt Publishing.
50. Yarger, R.H. (2008). *Towards a Theory of Strategy: Art Lykke and the Army War College Strategy Model*, www.au.af.mil/ au/awc/awcgate/army-usawc/stratpap.htm, retrieved on 14 March 2024.

SECURITY RISKS BETWEEN ANALYSIS AND ASSUMPTIONS

Lieutenant Colonel Carmen-Maria MOISE, PhD
Defence Staff
Irina TĂTARU, PhD
"Carol I" National Defence University, Bucharest
DOI: 10.55535/RMT.2024.4.29

The identification, analysis and management of security risks is a real challenge for any state, especially in the current geostrategic context. All of them belong to the risk management process and cannot be left to assumptions, but require a specialized approach by people with expertise in the field. No developed state can afford to leave security risks to chance, because it can cost its very existence as a sovereign and independent state.

In the current security environment, the lack of a correct risk analysis can lead to a weakening of the administrative capacity to respond to new forms of regional or international security threats. In its absence, the state will not be able to take appropriate measures and will not be able to take the necessary actions to protect its interests in the face of vulnerabilities of any type. A careful and in-depth analysis can facilitate the reduction of exposure to different types of risk, resulting in minimizing the negative effects determined by the possible manifestation of the identified security risks. However, risk identification is only a primordial stage in the complex process of risk management.

Keywords: risk; security environment; risk management; communication services; administrative capacity;

INTRODUCTION

Why Security Risk Management? Security risk management is a topic extensively addressed and debated both in the media and official documents, ranging from Romania's National Defence Strategy to various risk registers within public organizations. At times, it may seem overly discussed or even insignificant. However, we believe otherwise. On the contrary, improperly managed security risks lead to organizational decline and, on a larger scale, to the administrative decline of a country, causing a decrease in credit ratings, economic performance, and, in some cases, creating hard-to-repair security breaches.

Even though this subject is widely discussed, debated, and written about, we question whether these risks are managed scientifically within Romania's public entities or if the process is mostly formalism, relying on opinions and assumptions without a solid scientific foundation. It would be intriguing to determine how much of the approach is based on science versus formalism. It would be a significant challenge and difficult to ascertain.

Public entities collectively form the administrative system of the state – its organism. Administrative capacity can be compared to the body's functioning. Good administrative capacity thus reflects a healthy organism. Just as we strengthen the immune system for colder seasons, enhancing administrative capacity must be a priority for any state seeking to counter threats or vulnerabilities to its security.

But how can this be achieved for security risks? What mechanisms and measures ensure the proper functioning of the risk management process in this context? To answer these questions, we have conducted an analysis of documents from other NATO member states to gain an overview of how they manage security risks. We believe that, by adopting examples already implemented in more developed countries and systematically applying them, an organizational culture in this area can be developed.

RISK ANALYSIS IN MOST IMPORTANT NATIONAL DOCUMENTS

Unsurprisingly, this aspect of administrative capacity of managing risks closely tied to public finance management, is identified as a primary vulnerability in Romania's National Defence Strategy for 2020-2024: *"The capacity of state institutions to evaluate and mitigate the impact of risks and threats is limited by the persistence of vulnerabilities in the allocation and management of public funds, as well as in accessing European funds (including those under the 2021-2027 Multiannual Financial Framework); the regulation and organization of essential sectors such as health and education; the development and implementation of public policies."* (National Defence Strategy, 2020, p. 29). Interestingly, this document acknowledges a limited administrative capacity to manage risks due to these vulnerabilities.

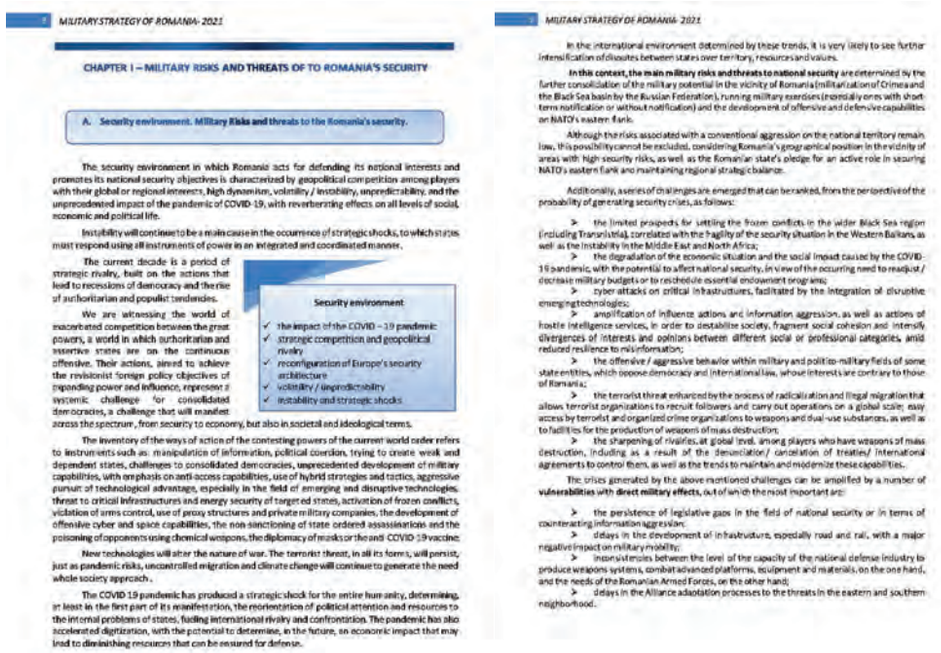
Returning to this aspect, for good risk management, a scientific and professional approach is needed, as well as promptness in determining them. As outlined in the National Defence Strategy for 2020-2024, Romania faces various security risks, including: *"1. The so-called illiberal temptation; 2. The evolution of the Republic of Moldova represents a risk, due to the prospect of counterbalancing the European orientation; 3. The indefinite stagnation of EU enlargement in the Western Balkans; 4. Risks to EU and NATO states from the south; 5. The increasing fragmentation of the international order and the decline of multilateralism; 6. The absence of real multiannual budgetary planning; 7. The persistence of inadequate infrastructure, a deficit in specialized resources, and underfunding; 8. Illegitimate actions undertaken by interest groups; 9. Ongoing dysfunctions in the organization of major public systems (health, education, and social assistance); 10. Intensification of Islamist-jihadist propaganda; 11. The accentuation of demographic decline; 12. Economic challenges, perpetuation of the shadow economy and corruption; 13. Difficulties in managing European funds; 14. The risk of losing cultural heritage; 15. Organized crime groups; 16. Extremist actions; 17. The use of new technologies; 18. Dependence on a limited number of technology providers for communication services; 19. The risk of triggering an interstate armed conflict remains low, but the risk of adapting hybrid offensive operations is looming"*. (Ib., p. 27).

Many of the mentioned aspects can be considered risks according to the theoretical definition, uncertain events likely to occur in the future. However, others are no longer risks, but unresolved problems or manifested risks, which were once in the category of risks, but were not managed well enough to not manifest, such as: *"Persistence of poor infrastructure, shortage of specialized resources and underfunding; Absence of real multiannual budgetary planning; Accentuation of demographic decline".* (Ib.).

According to the same document, Romania also faces additional *"sources of risks"*, which are represented by:

- *"Re-evaluation of arms control regimes, rising defence budgets, and accelerated development of military capabilities by state actors;*
- *Volatility in the security situation in the Western Balkans, along with unresolved conflict hotspots in the broader Black Sea region and limited prospects for resolving frozen conflicts in the region, compounded by a lack of transparency regarding Russian weaponry stationed in the separatist Transnistrian region and prolonged security crises in eastern Ukraine, triggered by the illegal annexation of Crimea;*
- *Phenomena with low probability but with major impact: low-intensity military confrontations, but persistent over time; massive influx of migrants; ecological disasters, natural catastrophes; aggressions against the quality of environmental factors or other calamities."* (Ib.).

Another important national document referencing security risks is the Military Strategy of Romania. We believe that it should address risk management aspects. If significant risks are not included, likely due to public policy decisions we cannot analyse here, such omissions are noteworthy. For instance, in Chapter I – Risks and Military Threats to Romania's Security (Military Strategy of Romania, 2021, p. 7), while the title mentions *"risks"*, no specific risks are described. Instead, the causes that could generate risks and the geopolitical context are described! The latter represent, from a scientific point of view related to risk management, the aspects that must be taken into account in identifying a risk. From the text, we can infer the possibility of a low-probability armed conflict on Romanian territory, but no more than that!



MILITARY STRATEGY OF ROMANIA- 2021

CHAPTER I – MILITARY RISKS AND THREATS OF TO ROMANIA'S SECURITY

A. Security environment. Military Risks and threats to the Romania's security.

The security environment in which Romania acts for defending its national interests and promotes its national security objectives is characterized by geopolitical competition among players with their global or regional interests, high dynamism, volatility / instability, unpredictability, and the unprecedented impact of the pandemic of COVID-19, with reverberating effects on all levels of social, economic and political life.

Instability will continue to be a main cause in the occurrence of strategic shocks, to which states must respond using all instruments of power in an integrated and coordinated manner.

The current decade is a period of strategic rivalry, built on the actions that lead to recessions of democracy and the rise of authoritarian and populist tendencies.

Security environment
- ✓ the impact of the COVID – 19 pandemic
- ✓ strategic competition and geopolitical rivalry
- ✓ reconfiguration of Europe's security architecture
- ✓ volatility / unpredictability
- ✓ instability and strategic shocks

We are witnessing the world of exacerbated competition between the great powers, a world in which authoritarian and assertive states are on the continuous offensive. Their actions, aimed to achieve the revisionist foreign policy objectives of expanding power and influence, represent a systemic challenge for consolidated democracies, a challenge that will manifest across the spectrum, from security to economy, but also in societal and ideological terms.

The inventory of the ways of action of the contesting powers of the current world order refers to instruments such as: manipulation of information, political coercion, trying to create weak and dependent states, challenges to consolidated democracies, unprecedented development of military capabilities, with emphasis on anti-access capabilities, use of hybrid strategies and tactics, aggressive pursuit of technological advantage, especially in the field of emerging and disruptive technologies, threat to critical infrastructures and energy security of targeted states, activation of frozen conflicts, violation of arms control, use of proxy structures and private military companies, the development of offensive cyber and space capabilities, the non-sanctioning of state ordered assassinations and the poisoning of opponents using chemical weapons, the diplomacy of masks or the anti-COVID-19 vaccine.

New technologies will alter the nature of war. The terrorist threat, in all its forms, will persist, just as pandemic risks, uncontrolled migration and climate change will continue to generate the need whole society approach.

The COVID-19 pandemic has produced a strategic shock for the entire humanity, determining, at least in the first part of its manifestation, the reorientation of political attention and resources to the internal problems of states, fueling international rivalry and confrontation. The pandemic has also accelerated digitization, with the potential to determine, in the future, an economic impact that may lead to diminishing resources that can be ensured for defense.

MILITARY STRATEGY OF ROMANIA- 2021

In the international environment determined by these trends, it is very likely to see further intensification of disputes between states over territory, resources and values.

In this context, the main military risks and threats to national security are determined by the further consolidation of the military potential in the vicinity of Romania (militarization of Crimea and the Black Sea basin by the Russian Federation), running military exercises (especially ones with short-term notification or without notification) and the development of offensive and defensive capabilities on NATO's eastern flank.

Although the risks associated with a conventional aggression on the national territory remain low, this possibility cannot be excluded, considering Romania's geographical position in the vicinity of areas with high security risks, as well as the Romanian state's pledge for an active role in securing NATO's eastern flank and maintaining regional strategic balance.

Additionally, a series of challenges are emerged that can be ranked, from the perspective of the probability of generating security crises, as follows:

- ➢ the limited prospects for settling the frozen conflicts in the wider Black Sea region (including Transnistria), correlated with the fragility of the security situation in the Western Balkans, as well as the instability in the Middle East and North Africa;
- ➢ the degradation of the economic situation and the social impact caused by the COVID-19 pandemic, with the potential to affect national security, in view of the occurring need to readjust / decrease military budgets or to reschedule essential endowment programs;
- ➢ cyber attacks on critical infrastructures, facilitated by the integration of disruptive emerging technologies;
- ➢ amplification of influence actions and information aggression, as well as actions of hostile intelligence services, in order to destabilize society, fragment social cohesion and intensify divergences of interests and opinions between different social or professional categories, amid reduced resilience to misinformation;
- ➢ the offensive / aggressive behavior within military and politico-military fields of some state entities, which oppose democracy and international law, whose interests are contrary to those of Romania;
- ➢ the terrorist threat enhanced by the process of radicalization and illegal migration that allows terrorist organizations to recruit followers and carry out operations on a global scale; easy access by terrorist and organized crime organizations to weapons and dual-use substances, as well as to facilities for the production of weapons of mass destruction;
- ➢ the sharpening of rivalries, at global level, among players who have weapons of mass destruction, including as a result of the denunciation / cancelation of treaties/ international agreements to control them, as well as the trends to maintain and modernize these capabilities.

The crises generated by the above-mentioned challenges can be amplified by a number of **vulnerabilities with direct military effects**, out of which the most important are:

- ➢ the persistence of legislative gaps in the field of national security or in terms of counteracting information aggression;
- ➢ delays in the development of infrastructure, especially road and rail, with a major negative impact on military mobility;
- ➢ inconsistencies between the level of the capacity of the national defense industry to produce weapons systems, combat advanced platforms, equipment and materials, on the one hand, and the needs of the Romanian Armed Forces, on the other hand;
- ➢ delays in the Alliance adaptation processes to the threats in the eastern and southern neighborhood.

Image 1: Risks and threats of a military nature to Romania's security
(Military Strategy of Romania, ib.)

Continuing with Romania's important documents, we find the *White Paper on Defence*[1], which, according to the Defence Planning Law no. 203/2015, is the departmental-level defence planning document aimed at fulfilling the provisions of the National Defence Strategy and implementing the defence objectives established by the Government Program. The *White Paper* is developed by the Ministry of National Defence, endorsed by the Government of Romania, approved by the Supreme Council of National Defence, and adopted by Parliament, as stipulated by law, for a four-year horizon. In this document, we find, on page 12, the section on Risks and Threats. Upon closer analysis, we can observe that the main risks and threats, as well as their causes, are not clearly delineated. There is mention of the risk of a major conflict, which, in 2021, was categorized as a low-level risk – meaning the probability of such a conflict was considered minimal. We can also deduce the potential occurrence of cyberattacks, identified as possible threats, but there is no identification of potential risks in this area.

[1] Hotărârea nr. 28 din 11 mai 2021 a Parlamentului României, pentru aprobarea *Cartei Albe a Apărării*/Romanian Parliament Decision no. 28 on 11 May 2021 to adopt the *White Paper on Defence*, published in the *Official Gazette of Romania*, Part I, no. 499/13 May 2021.

As we now know, an armed conflict of uncertain duration is currently unfolding near Romania: *"On 24 February 2022, Russia invaded Ukraine, escalating the Russo-Ukrainian war that began in 2014. The invasion, the largest conflict in Europe since World War II, has caused hundreds of thousands of military casualties and tens of thousands of Ukrainian civilian casualties. By 2024, Russian forces occupied approximately 20% of Ukraine's territory. Out of a population of 41 million, about 8 million Ukrainians were internally displaced, and over 8.2 million left the country by April 2023, creating the largest refugee crisis in Europe since World War II"*[2].

In the previously mentioned documents, we observe inconsistencies in the description of risks and cannot identify a clear separation between risks, vulnerabilities, and threats. This simple textual analysis reveals a beginner-level approach to risk management, which, we believe, will not create future opportunities but rather vulnerabilities. This is precisely why we believe it is necessary to develop an organizational culture within public entities, especially in those belonging to the National Security System, that employs advanced risk management practices.

In this context, the examples from other countries that have been utilizing this process for a long time can serve as valuable resources. For illustration, we will mention diverse approaches found in the national documents of the United States of America and the United Kingdom. The snapshots from these documents, identified online, are considered representative and necessary to present for understanding the importance these countries place on risk management.

RISK MANAGEMENT IN DOCUMENTS FROM OTHER NATO MEMBER STATES – USA AND UK

The US National Defense Strategy 2022 (National Defense Strategy, 2022) contains an entire chapter – Chapter IX, page 22 of the introductory section – dedicated to risk management (Risk management/https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF). It highlights the importance of managing all types of risks and acknowledges the possibility of sometimes failing to identify all risks, which could lead to financial efforts being misdirected if risks are not correctly identified. Although not all risks are enumerated (as it is expected since they are the subject of more detailed documents, not the strategy itself), a few key risks are identified that would pose a real danger if intensified. The content emphasizes risks in the areas of cybersecurity and nuclear weapons (Ib.). We also observe the use of specific scientific terms

[2] Invazia Rusiei în Ucraina (2022–prezent)/Russia's invasion of Ukraine (2022-present), https://ro.wikipedia.org/wiki/Invazia_Rusiei_%C3%AEn_Ucraina_(2022%E2%80%93prezent), retrieved on 5 September 2024.

related to risk management, such as *"escalation risk"* (which occurs when a certain threshold is reached, either based on a time interval or another risk condition, thus requiring higher attention – for example, a risk left untreated for more than two fiscal periods might be flagged for additional controls. Another condition might arise if monitoring reveals that the risk exposure rating is expected to significantly exceed initial estimates (https://csrc.nist.gov/glossary/term/risk_escalation) and *"risk mitigation (the prioritization, evaluation, and implementation of appropriate controls/countermeasures recommended in the risk management process to reduce the impact of a risk"* (https://csrc.nist.gov/glossary/term/risk_mitigation*).*

Thus, it can be deduced that a comprehensive analysis was conducted prior to risk identification, and medium- and long-term measures were certainly proposed and outlined for managing these risks.

For a practical example of how risk identification is performed in other countries, we have chosen the United Kingdom model, which we consider very well-applied and organized. In the UK, at the governmental level, there is a public National Risk Register of Security Risks reflecting the National Security Risk Assessment (NSRA) (https://access-national-risk-register.service.cabinetoffice.gov.uk/risk-methodology). Also, on the governmental webpage, we find details on the identification process and can observe the teamwork behind this process.

HOW RISKS ARE IDENTIFIED AND EVALUATED FOR INCLUSION IN THE UK RISK REGISTER

First, risks are identified for inclusion in the NSRA through consultation with a broad range of experts from UK government departments, devolved administrations, the governmental scientific community, and external partners (such as partner agencies, academic institutions, and industry). Impact and probability assessments are conducted by specialized departments for each identified risk within their area of responsibility.

The next step is their classification through evaluation as *"reasonable worst-case scenarios".* These scenarios represent the most incorrect plausible manifestation of a specific risk (once highly unlikely variations are eliminated), enabling specialized entities to engage in proportional planning. Scenarios for each risk were developed in consultation with experts, with data collected from a wide range of sources.

The NSRA does not aim to capture every risk the UK might face. Instead, it seeks to identify a representative range of risks. The National Risk Register (NRR) is the public-facing version, essentially a snapshot of the NSRA, representing the government's assessment of the most severe risks facing the UK.

Not all risks are included in the register, only those that meet a certain *"tolerance threshold",* meaning those that could have a serious impact on the UK's safety, security, and/or critical infrastructures at the national level. The register includes 89 risks across nine risk themes – although many risks could be classified under multiple themes. These themes are: terrorism, cyber risks, state threats, geographic and diplomatic risks, accidents and system failures, natural and environmental risks, human, animal, and plant health risks, societal risks, and conflicts and instability.

The register presents the probability and impact of each risk, following a rigorous and well-tested methodology.

Risks can manifest in various ways, with varying levels of severity. To ensure the UK is prepared for a wide range of scenarios, the NRR establishes a *"reasonable worst-case scenario"* for each risk. It enables planning for all possible scenarios. Additionally, the register includes information on the capacities required for emergency response and recovery methods should a risk materialize.

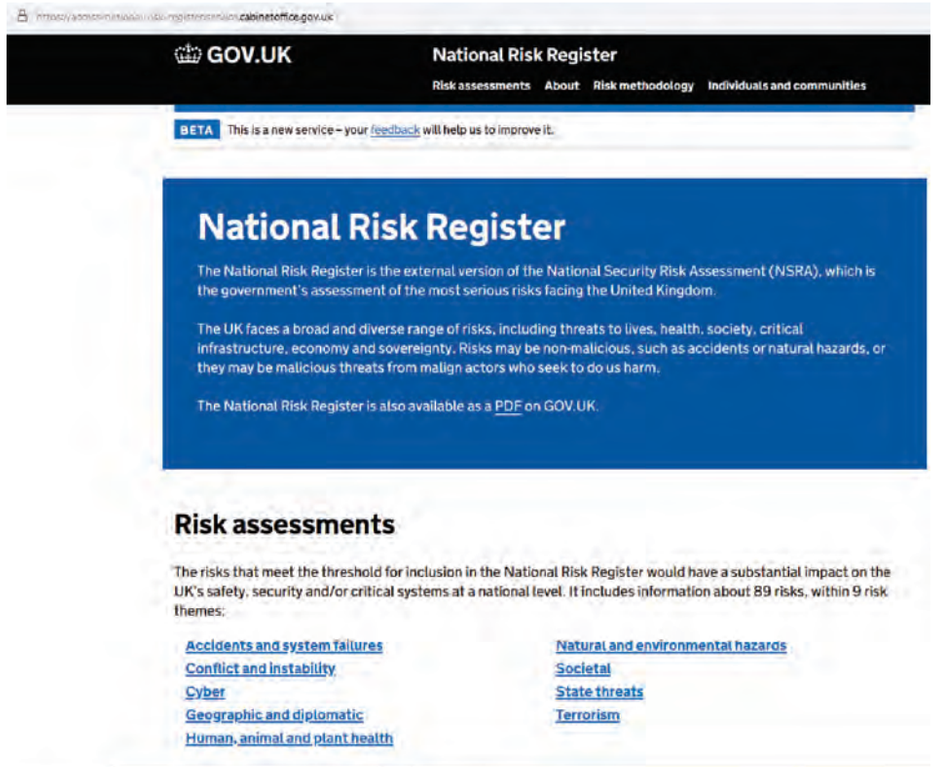


Image 2: The UK National Risk Register
(https://access-national-risk-register.service.cabinetoffice.gov.uk/, retrieved on 9 September 2024)

For example, we will present the probability and impact identified for a risk in the register, as well as how to frame the probability and impact according to different possible scenarios, subsequently leading to gradual measures depending on the resulting exposure.

▼ Impact & Likelihood

Impact key		Likelihood key	
5	Catastrophic	5	>25%
4	Significant	4	5-25%
3	Moderate	3	1-5%
2	Limited	2	0.2-1%
1	Minor	1	<0.2%

Image 3: How to determine likelihood and impact
(Geographic and diplomatic, https://access-national-risk-register.service.cabinetoffice.gov.uk/risk-themes/geographic-and-diplomatic, retrieved on 9 September 2024)



Image 4: Exposure to the risk "Disruption of Russian gas supplies to Europe" presented in the matrix used
(https://access-national-risk-register.service.cabinetoffice.gov.uk, retrieved on 11 September 2024)

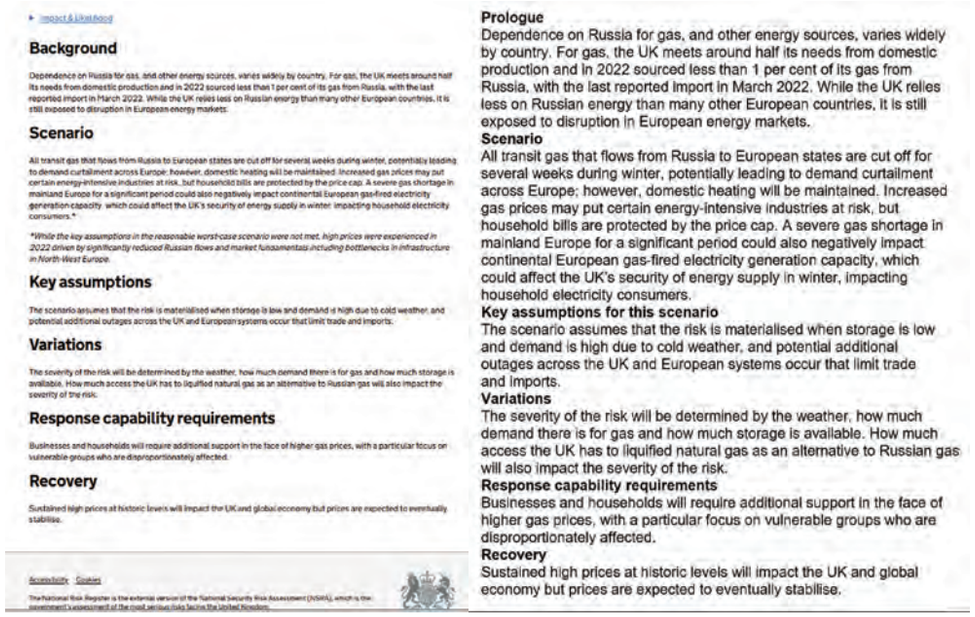


Image 5: Scenario and management of the materialization of the risk in Image 4
(Disruption of Russian gas supplies to Europe, https://access-national-risk-register.service.cabinetoffice.gov.uk, retrieved on 11 September 2024)

In the same platform created for the risk register, we find a grouping of risks identified by themes and a brief description of the management of each risk, depending on a possible scenario, with very easy access to the presentation of each risk, on the page called *"Risk Management"*[3].

IDENTIFICATION, ANALYSIS, AND MANAGEMENT OF SECURITY RISKS – A TRUE CHALLENGE

National security risks must be analysed and managed with the utmost care. It is every state's responsibility to issue coherent public policies that enable the creation of a strong state administration capable of handling various processes, whether simple or complex. Public entities within the national security system must receive increased attention and be allocated the necessary resources to effectively manage security risks. Primarily, human resources make the difference. Competent human resources always add value to any organization; however, they are the most challenging to attract, especially in the current economic context.

[3] *"Risk Management"* page in Risk Assessments (cabinetoffice.gov.uk), retrieved on 11 September 2024.

Risk scenarios

Sort by Risk ID Sort results

ID	Title	Risk Themes	Publishing date
1	International terrorist attack	Terrorism	July 2023
2	Northern Ireland related terrorism	Terrorism	July 2023
3	Terrorist attacks in venues and public spaces - explosive devices	Terrorism	July 2023
3	Terrorist attacks in venues and public spaces - marauding attacks	Terrorism	July 2023
4	Malicious aviation incident	Terrorism	July 2023
4	Malicious maritime incident	Terrorism	July 2023
4	Malicious rail incident	Terrorism	July 2023
5	Strategic hostage taking	Terrorism	July 2023
6	Assassination of a high profile public figure	Terrorism	July 2023
7	Smaller scale CBRN attacks	Terrorism	July 2023
8	Medium scale CBRN attacks	Terrorism	July 2023
9	Larger scale CBRN attacks	Terrorism	July 2023
10	Attack on government	Terrorism	July 2023
10	Conventional attack - civil nuclear	Terrorism	July 2023
10	Conventional attack - electricity infrastructure	Terrorism	July 2023
10	Conventional attack - fuel supply infrastructure	Terrorism	July 2023
10	Conventional attack - gas infrastructure	Terrorism	July 2023
10	Disruption of Russian gas supplies to Europe	Geographic and diplomatic	July 2023
10	Malicious attack on chemicals infrastructure	Terrorism	July 2023
10	Total loss of transatlantic telecommunications cables	State threats	July 2023

1 2 3 4 5 Next →

Image 6: How to access risks by topic and related scenarios

(Risk scenario, https://access-national-risk-register.service.cabinetoffice.gov.uk/risk-assessments, retrieved on 14 September 2024)

The primary goal is to maintain a strong and democratic state. In the risk management process, the correct identification of risks is crucial. We cannot proceed to analyse and manage risks with concrete and coherent measures unless we first succeed in correctly identifying them. According to specialists in the field, risks can be most easily identified through the cause-risk-effect formulation (Mulcahy, 2010, pp. 70-77). To pinpoint the cause(s), several techniques are recommended, the most commonly used being the question: *What if?*

Risk always pertains to the future, which is why it requires information resources, data connections, and complex analyses for accurate identification. Identified risks are not uncovered through revelations or premonitions but through thorough research.

It is also crucial to have constant resources that can be relied upon at any moment for risk identification. The stability of resources is essential; otherwise, the entire risk management process could be jeopardized.

In professional terminology, risks are defined as uncertain events that can positively or negatively impact objectives, projects etc. For this reason, risk management involves minimizing the consequences of negative events (threats) and maximizing the outcomes of potential positive events (opportunities) (Mulcahy, p. 3).

In any case, a risk exists when the percentage of certainty is far below 100% – otherwise, it becomes a fact or a problem, not a risk.

The risk management process itself involves a series of sub-processes. According to Rita Mulcahy, they can be summarized into seven:

1. Establishing institutional rules and policies for risk management or ***Risk Management Planning*** (It entails setting up the type of matrix to be used, defining the structure of the risk register and other necessary documents. Examples of methodologies and document templates can be found in Order no. M.100/ 13 May 2019, issued by the Minister of National Defence, approving the Methodological Norms for the internal managerial control system within the Ministry of National Defence, published in the *Official Gazette* no. 456/6 June 2019). This sub-process encompasses several key activities, illustrated in *Figure 1*:

2. Identification of risks through specific techniques, which we find described in the international standard SR EN 31010/2019 – Risk management. Risk assessment techniques, as well as in the specialized literature. This sub-process entails a series of main activities, presented in *figure 2*.



Figure 1: Establishing work rules and policies at the institutional level (authors' design)

3. Qualitative risk analysis which involves establishing a hierarchy of risks based on the estimated level of probability and impact. The main activities of this sub-process would be:

4. Quantitative risk analysis, a sub-process that involves a numerical analysis of the financial impact of risks. The main activities involved would be:

5. Developing the risk response plan, a sub-process that mainly involves establishing coherent and concrete measures to respond to the possible manifestation of risks. The main activities include:

6. Effective implementation of risk response measures, a complex sub-process that involves multiple activities to put into practice the measures established in response with allocated resources. The main activities are:

7. Risk monitoring and risk control, a sub-process that involves maintaining a state of vigilance and carefully monitoring any variations that could change the characteristics of a risk.

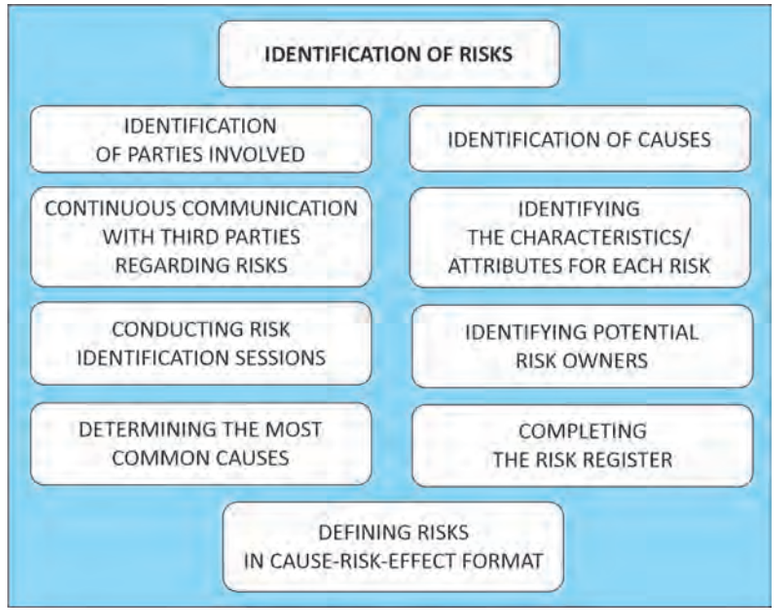


Figure 2: Risk identification (authors' design)

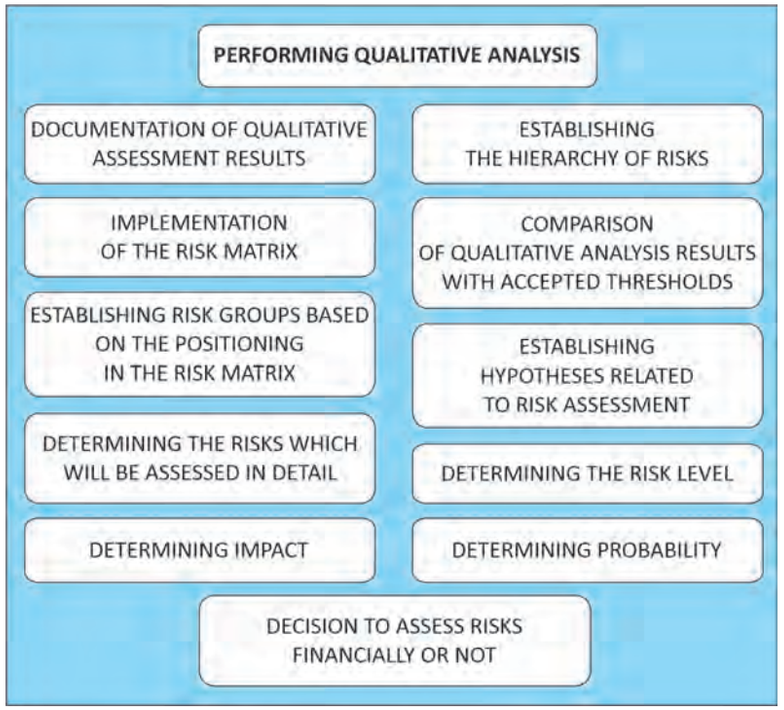


Figure 3: Qualitative risk analysis (authors' design)

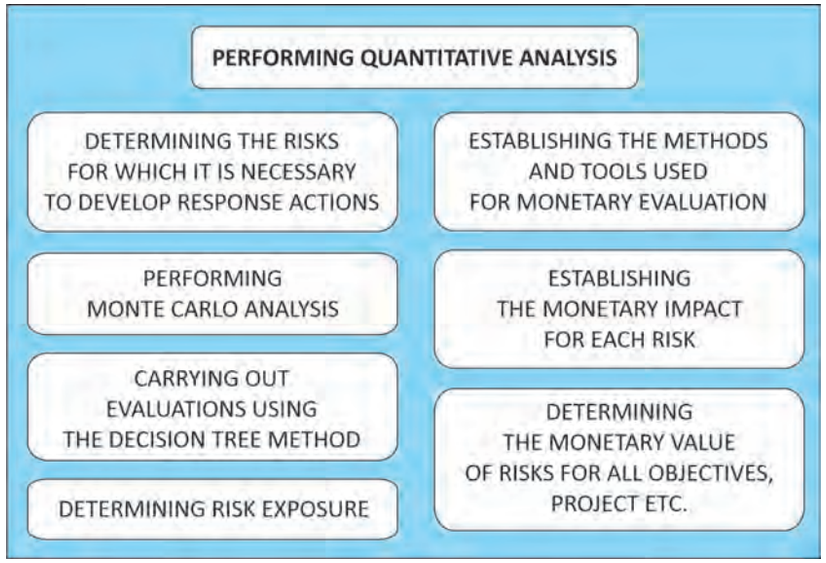


Figure 4: Quantitative risk analysis (authors' design)



Figure 5: Developing a risk response plan (authors' design)

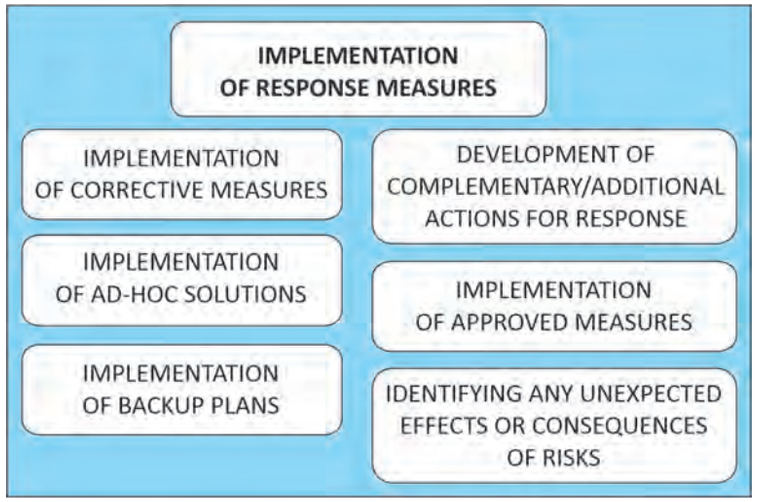


Figure 6: Effective implementation of risk response measures (authors' design)

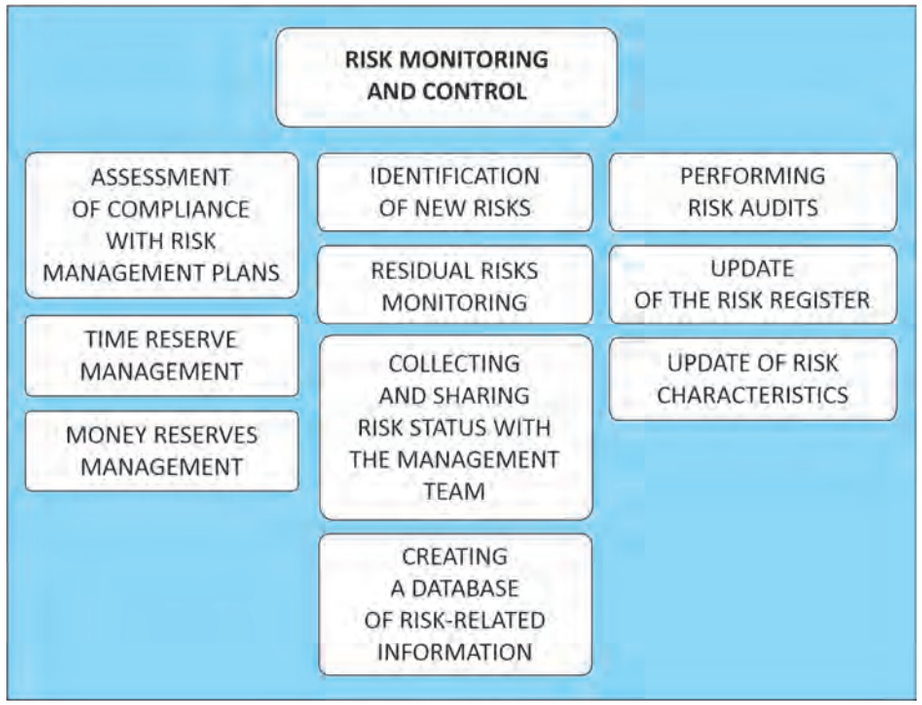


Figure 7: Risk monitoring and risk control (authors' design)

Each security risk, once identified, must go through all the necessary sub-processes to be considered and properly managed. Allocating access to multiple types of resources is a real challenge and must be prioritized not only

for identifying security risks but also for analysing and managing them. The complexity of this process requires teamwork and constant communication between the actors involved.

CONCLUSIONS

Risk management is the complex process of identifying, evaluating, and managing risks of all kinds, including security risks. Security risks arise from a variety of sources, such as financial uncertainties, technological issues, strategic management errors, accidents, and natural disasters, among others.

The safety of a country lies in its ability to respond to the potential manifestations of identified security risks. For this reason, we believe that continuous preparation through plans, projects, and strategies is a vital necessity for the public administration of any country.

A well-structured risk management program helps to account for the full spectrum of risks a country might face and is implemented in all developed nations around the world. Such programs aid in identifying complex processes that require attention in order to prepare, in advance, the most appropriate response to risks.

Today, more than ever, thanks to the internet, the media, and rapid mobility between states, a risk manifested in one country can easily manifest shortly thereafter in another. For example, risks related to public health issues such as various diseases, or cybersecurity risks. It makes professional risk management all the more necessary and desirable. Risk management is directly influenced by the professionalism of human resources. Human resources should be the **number one priority** of any nation.

The implementation of clear and consistent policies promoting proper risk management is an essential step toward creating a cohesive approach to national security. Establishing and sustaining a risk management culture requires continuous commitment and support. The development of risk management capabilities demands time, resources, training, and ongoing support from top-level managers, adhering to the much-cited principle of the "*Tone of the Top"*[4]*.*

The examples and analyses presented in this text provide a practical demonstration of the necessity and benefits of prioritizing security risk management. Risk management plays a crucial role in achieving the objectives of entities of any kind and aids in identifying risks that may sometimes present

[4] *The first ingredient in a world-class ethics and compliance program Tone at the Top*, https://www2.deloitte.com/us/en/pages/risk/articles/tone-at-the-top-the-first-ingredient-in-a-world-class-ethics-and-compliance-program.html, retrieved on 17 September 2024.

opportunities. International standards in the field ensure the use of a universally accepted terminology.

There are numerous benefits to utilizing this process, such as: preparing in advance for potential adverse events and/or opportunities, making well-informed, strategic decisions. Top managers of any organization must constantly take into account potential risks that could impact their established objectives.

The consequences of poor risk management in public administration will directly affect the responsiveness of state entities. These consequences can sometimes be disastrous, leading to the failure of projects, strategies, or actions.

BIBLIOGRAPHICAL RESOURCES:

1. Computer Security Resource Center, https://csrc.nist.gov/glossary/term/risk_escalation, retrieved on 3 September 2024.
2. *Escalation risk*, in Computer Security Resource Center, https://csrc.nist.gov/glossary/term/risk_escalation, retrieved on 3 September 2024.
3. *Hotărârea nr. 28 din 11 mai 2021 a Parlamentului României, pentru aprobarea Cartei Albe a Apărării/Parliament Decision no. 28 on 11 May 2021 to adopt the White Paper on Defence*, published in the Official Gazette of Romania, Part I, no. 499/13 May 2021.
4. *Invazia Rusiei în Ucraina (2022–prezent)/Russia Invasion in Ukraine (2022-present)*, https://ro.wikipedia.org/wiki/Invazia_Rusiei_%C3%AEn_Ucraina_(2022%E2%80%93prezent), retrieved on 5 September 2024.
5. Mulcahy, R. (2010). *Risk Management Tricks of the Trade for Project Managers*.
6. National Defence Strategy 2022, https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF, retrieved on 5 September 2024.
7. *National Risk Register*, https://assets.publishing.service.gov.uk/media/64ca1dfe19f5622669f3c1b1/2023_NATIONAL_RISK_REGISTER_NRR.pdf, retrieved on 6 September 2024.
8. *Risk assessment methodology*, https://access-national-risk-register.service.cabinetoffice.gov.uk/risk-methodology, retrieved on 6 September 2024.
9. *Scenario in the event of a nuclear attack*, https://access-national-risk-register.service.cabinetoffice.gov.uk/risk-scenario/2817, retrieved on 11 September 2024.
10. SR ISO 31000/2018 – *Managementul riscurilor. Principii şi linii directoare*, https://www.asro.ro/a-aparut-sr-iso-31000-managementul-riscului/, retrieved on 11 September 2024.
11. SR EN 31010/2019 – *Managementul riscului. Tehnici de evaluare a riscurilor*, https://www.iso.org/standard/72140.html, retrieved on 12 September 2024.
12. *Strategia Militara a României/Military Strategy of Romania* (2021). București: Ministerul Apărării Naționale.
13. *Strategia Națională de Apărare a Țării pentru perioada 2020-2024/National Defence Strategy* (2020). București: Administrația Prezidențială.
14. https://www2.deloitte.com/us/en/pages/risk/articles/tone-at-the-top-the-first-ingredient-in-a-world-class-ethics-and-compliance-program.html, retrieved on 17 September 2024.

THE KOSOVO PRECEDENT – SIMILAR EFFECTS ON OTHER STATES – CASE STUDY: GEORGIA AND UKRAINE

Ioan-Sebastian BUDUROI, PhD Student
"Alexandru Ioan Cuza" University, Iaşi
DOI: 10.55535/RMT.2024.4.30

Kosovo, the battlefield of the last major conflict in the Yugoslav Wars, has undergone radical ethnic changes over the centuries, resulting in inter-ethnic tensions that are still felt today. A region rich in culture, history and minerals, whose hilly configuration forms a logistically defensible border for southern Serbia, Kosovo finds itself in a diplomatic stalemate over the non-recognition of the full independence declared by the Albanian majority in the Republic of Kosovo.

Using the Kosovo precedent, Russia is trying to legitimise its own actions that violate the sovereignty and territorial integrity of Georgia and Ukraine. These are the main aspects that are discussed in the present study, employing the case study of Georgia and Ukraine.

Keywords: Kosovo; legitimacy; Georgia; Ukraine; conflict;

INTRODUCTION

The world wars of the first half of the last century seemed to convince the West that Europe would prosper in peace and tranquillity after the end of the Second World War, given the first-ever transcontinental alliances on the scale of NATO or the European Community. That remained the case until the last decade of the 20th century, when the entire international community was rocked by a series of bloody wars, genocides and ethnic cleansings, reminding humanity of the horrors of the previous world wars. On the European continent, only Yugoslavia experienced a transition from dictatorial communism to quasi-democracy marked by a particularly violent state disintegration caused by several interethnic wars that engulfed almost the entire country (Chomsky, Džalto, Grubačić, 2018, p. 50).

The Kosovo War was the last of these wars, beginning in 1998 and ending a year later with the signing of the Kumanovo Agreement. The latter failed, however, to put a definitive end to the notable inter-ethnic tensions, as there is a perpetual fear in the international community that such a simmering conflict could at any moment turn into a new full-scale war between the two peoples claiming sovereignty over the territory, namely Albanians and Serbs (38 I.L.M. 1217, 1999, art. II; Cox, 2002, pp. 170-171).

Highlighting that Kosovo's unilateral declaration of independence is not a *sui generis* case, this paper employs the case study method, implementing a multiple-case design and using the comparative synthesis technique to demonstrate the effects of the Kosovo precedent on other states. It focuses on the consequences felt by Georgia and Ukraine due to Russia's instrumentalisation of Kosovar secession.

Kosovo, Serbia's southernmost province, is geographically varied, with hilly plains, mineral-rich mountains and fertile, often overworked soils. A popular chant among Serbs is *"Kosovo je srce Srbije/Kosovo is the heart of Serbia"*, and this is true, at least when looking at the history of medieval Serbia. Over time, however, the territory has become the centre of an endless dispute between Serbs and Albanians. The many significant battlefields, churches, monasteries, and palaces remind locals and visitors alike that the history of medieval Serbia was grand. However, historians believe that the province of Kosovo was probably never one in which Serbs enjoyed ethnic exclusivity. At least since the 17th century, Kosovo has undergone constant demographic changes. It explains how the Serbs have become a negligible minority

in this vital region, even though they used to represent the absolute majority of the province's population.

The majority Albanian population began to resist the Serbian administration of the province by a variety of means as soon as the Serbs succeeded in driving out the Turks in 1913, after a long period of Ottoman occupation. A third of the world's Albanian population now lives in Kosovo. For example, while Albania's population barely exceeds three million, Kosovo is home to more than one and a half million Albanians. The province has remained the most underdeveloped in former Yugoslavia, despite massive investment by Yugoslav governments in local industry, and its gross domestic product *per capita* was the lowest in the whole of Yugoslavia.

The present is even bleaker as a direct result of the political repression and violence in the province's recent past. Whereas until the collapse of Yugoslavia's communist regime, many Albanians wanted a greater degree of autonomy within Serbia, today, almost the entire Albanian population of Kosovo aspires to independence. Conversely, the Serbs rule out any possibility of definitively relinquishing control over the province. Apart from its cultural importance and abundance of minerals, the province's hilly configuration is also strategically important to the Serbian state, as Kosovo forms a border through which the Serbs can easily defend the country's south logistically (Cox, 2002, pp. 6-7).

THE PATHWAY TO INDEPENDENCE: THE KOSOVO WAR AND RESOLUTION 1244

In 1991, the Kosovo Liberation Army (KLA), an Albanian group with terrorist origins, was formed. Five years later, it began a series of armed attacks and assassinations on Serbs, whether civilians or government officials. Moreover, the KLA also targeted ethnic Albanians considered to be *"collaborators with the Belgrade regime".* However, the group's first act of terrorism was in 1993 when it claimed responsibility for the murder of two Serb policemen in the very centre of the Kosovo province. A vehement reaction from the Serbian government did not come until 1998 when the KLA killed several Serbian policemen, ambushed in another terrorist attack. Realising that the KLA's inexorable violence would not go away on its own but would escalate unless action was taken, Serbian policemen decided to respond with retaliation by storming a village in Drenica, where they suspected members of the group who were responsible for organising the ambush were living. The fact that Albanian press reports interpreted the Serbian police actions as atrocities committed against Albanian civilians only served to attract a considerable

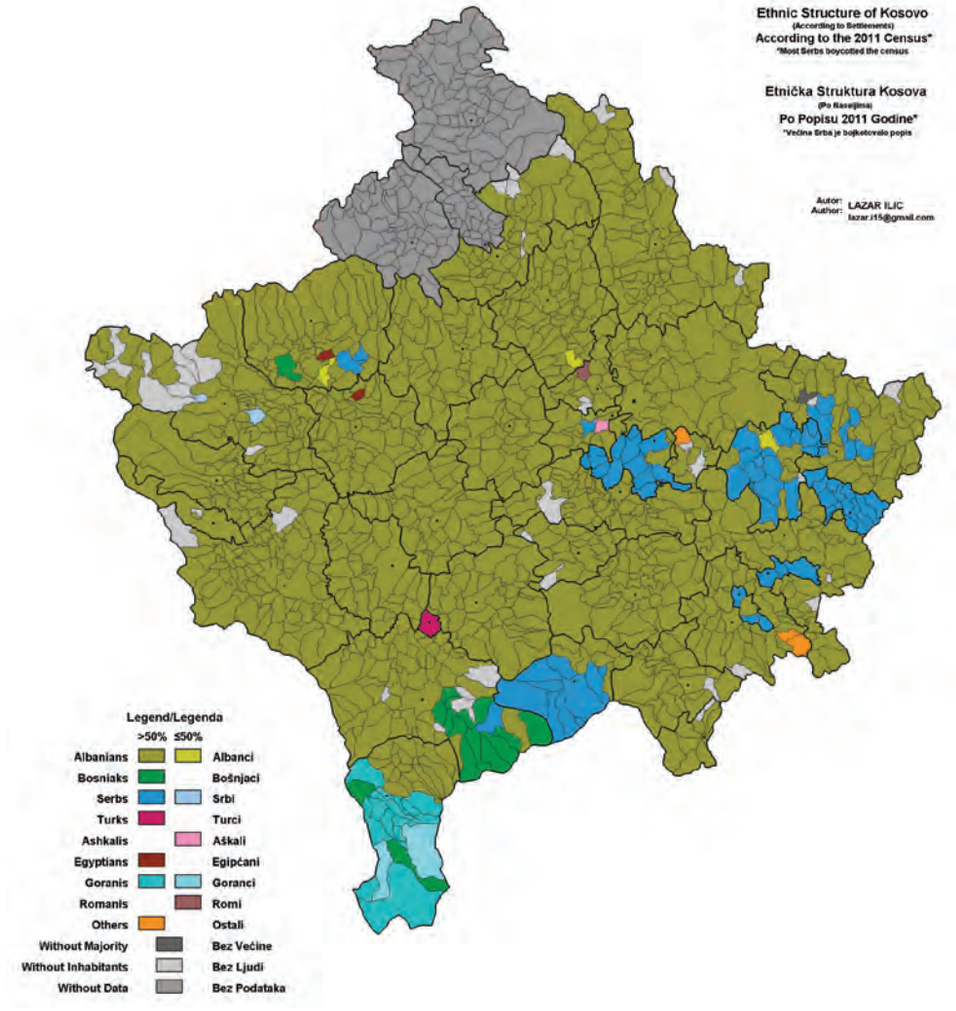


Figure 1: Ethnic map of Kosovo according to the 2011 census (Ilic, 2013)

number of fighters to the KLA. The events in Drenica are thus considered the starting point for the Kosovo War (Achcar, 2023, p. 103; Castan Pinos, 2019, p. 24; Cox, 2002, pp. 166-167; Dietrich, 2010, p. 125; Fella, 2024, p. 10). In the fall of 1998, following the adoption by the United Nations Security Council (UNSC) of Resolution 1203, which called for the withdrawal of Serbian troops from Kosovo and the start of negotiations between Serbs and Albanians, Milošević accepted the proposal of Richard Holbrooke, US Special Envoy to the Balkans, to withdraw 10.000 Serbian troops from Kosovo and to accept the deployment of 2.000 Kosovo Verification Mission (KVM) members by the Organisation for Security and Cooperation in Europe

(OSCE). However, the KLA refused to comply with this UNSC decision, and the war continued (Achcar, 2023, pp. 104-105; Dietrich, 2010, p. 125).

The official US position changed drastically in just a few months since the war began. While the Clinton administration had initially accused the KLA of being nothing more than another terrorist organisation, given its war crimes and the fact that many of its members constituted a *de facto* organised criminal group with, among other concerns, activities such as drug and human trafficking, kidnappings and rape, US officials changed their minds. Suddenly, the KLA became, according to the new US narrative, a military group with the legitimacy to fight against the oppressive Serbian regime (Castan Pinos, 2019, pp. 30-32; Visoka, 2018, pp. 64-66). The media continued to report only the crimes attributed to Serbian troops against the Albanian population, ignoring the fact that these Serbian actions were a direct consequence of violent provocations by Albanian militants and the flagrant and repeated violations of the ceasefire by the KLA. Thus, the West became increasingly hostile towards the Belgrade regime led by Slobodan Milošević, culminating in NATO's bombing of Serbia, starting on 24 March 1999, labelling the intervention as humanitarian, with the official objective of putting an end to Serbian operations of ethnic cleansing of the Albanian majority in Kosovo. The fact that NATO took this decision without obtaining UN permission further angered the Serbian public, resulting in a furious rise in support for Milošević. The Serbs' grievance was that the West was biasedly violating the sovereignty of their state in the name of human rights since both the KLA terrorist attacks and the mass expulsion of Serbs from Croatia only four years earlier went unpunished. The NATO bombing campaign against Serbia lasted 78 days, during which more than 23.000 bombs and rockets were dropped, killing up to 3.000 civilians and soldiers and destroying the entire infrastructure of the country. On the other side, the Serbs did not kill a single NATO soldier.

Initially, the objectives of the bombing campaign were strictly military. Nevertheless, Milošević's refusal to sue for peace turned the campaign's goal into the destruction of civilian morale in order to bring down the regime or achieve peace. It was not only Serbs who were angered by the numerous NATO attacks on civilians, but even some citizens of NATO member states. Almost the entire international community has expressed its disapproval of NATO's aggression against former Yugoslavia since its bombing campaign against the Serbs was a flagrant violation of the prohibition on the use of force. However, Western tactics paid off, and the Serbs eventually signed the Kumanovo Agreement, officially ending NATO's bombing of Serbia on 10 June, the day on which UN Resolution 1244 was adopted.

The resolution reaffirmed Serbia's (then still the Federal Republic of Yugoslavia) sovereignty over Kosovo. It also authorised the deployment of 50.000 KFOR troops to oversee the region's autonomy from the Serbian government and ensure peace. Another important provision was the temporary withdrawal of all Serbian troops from Kosovo, whether military or police. Finally, the Kosovo War was thus coming to an end (38 I.L.M. 1217, 1999, art. II; Baranovsky, 2015, p. 279; Castan Pinos, 2019, pp. 39, 55-56, 73-74; Cox, 2002, pp. 168-170; Dietrich, 2010, pp. 125-126; Dugard, 2013, p. 204; Escudero Espinosa, 2017, p. 108; Fella, 2024, p. 10; Ingimundarson, 2023, pp. 185, 187; Jelesijević, 2023, pp. 29, 31; UNSCR 1244, 1999; Visoka, 2018, pp. 64-66).

UNILATERAL DECLARATION OF INDEPENDENCE: CONTEXT, RECOGNITION AND LEGITIMACY

Over the last 250 years, the development of international law has been marked by the process of state recognition, which began as early as the 17th-18th centuries, when the establishment of diplomatic relations confirmed the mutual recognition of the existence of states. The principle of self-determination, however, gave rise to the process of recognising states' *de jure* independence at the same time as they obtained their *de facto* independence. To date, international law has not formally regulated this process. As a result of the lack of such regulations, states worldwide are increasingly using the withdrawal of recognition of independence as a tool to undermine the legitimacy and international legal personality of states that have unilaterally declared their independence. In this regard, the first historical example was Taiwan. Even if the recognition of the world's states is not among the legal competencies of the UN, their membership in the organisation is often tantamount to acquiring *de jure* universal recognition of independence (Cakolli, 2020, pp. 4, 10).

The 1933 Montevideo Convention established four criteria that the states of the world must fulfil in order to become international legal personalities: they must have a permanent population, a well-defined territory, they must be governed, and maintain diplomatic relations with other states (art. 1). Although the convention originally had regional applicability, its criteria for statehood have come to be accepted as definitive worldwide, not only by jurists and lawyers but, more importantly, by the states of the world. Thus, the Montevideo Convention's criteria now constitute the legal conditions for statehood that states must consider when deciding whether to recognise a separatist entity's independence (Dugard, 2013, p. 27). Whereas at the beginning of the last century, only about 50 states were recognised worldwide, the number of internationally recognised states is now

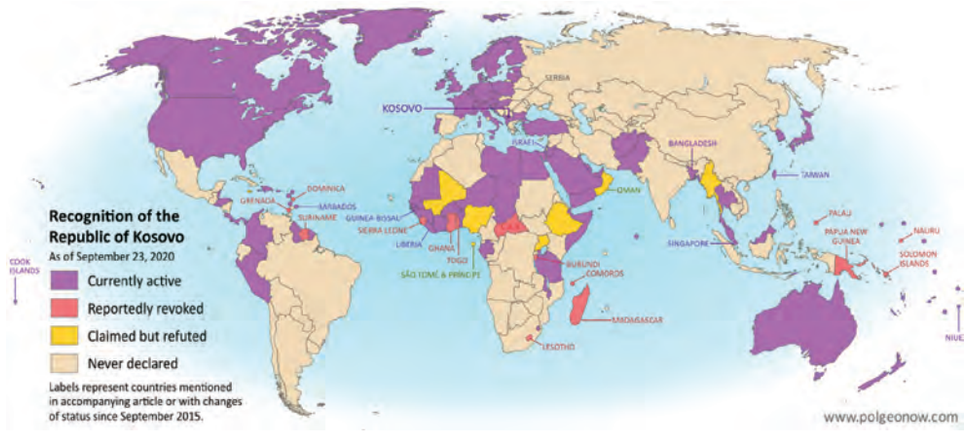


Figure 2: World map of states according to their recognition status of Kosovo's independence (Centanni, 2020)

almost four times higher. The decolonisation process that followed the Second World War alone led to the establishment and recognition of the independence of more than 100 states, a period that would go down in history as the *"era of secessionism"*. The disintegration of the Soviet Union, Yugoslavia, and Czechoslovakia in the 1990s also significantly contributed to the current 193 UN member states. However, apart from the colonial context, states that gained their independence through secession and became UN members belong to a select club since the organisation often opposes secession without the consent of national governments. Bangladesh, Eritrea, South Sudan and, of course, Croatia and Bosnia and Herzegovina are exceptions to the rule (Cakolli, 2020, p. 7; Dugard, 2013, pp. 32, 156-158).

Closely watched by the USA and the most prominent EU member states, the so-called Republic of Kosovo unilaterally declared its independence from Serbia on 17 February 2008, yet another action taken without UNSC consent (Achcar, 2023, p. 152; Almqvist, 2013, p. 180; Boguslaw, 2020, p. 721; Castan Pinos, 2019, pp. 103-104; Dietrich, 2010, pp. 123, 127; Dugard, 2013, p. 205; Džihić, Kramer, 2009, pp. 4-5; Fella, 2024, pp. 14-15; Ingimundarson, 2023, p. 187; Jelesijević, 2023, pp. 30-31; Kosovo Declaration of Independence, 2008; Newman, Visoka, 2018, p. 372; Nte, 2023, p. 5; Richter, Halbach, 2009, p. 223; Visoka, 2018, p. 73). Although initially not even a third of the Kosovar Albanian population identified with the symbols of the new state, less than a decade after the declaration of independence, suddenly, the entire Albanian population of the province began to adore the flag and state anthem of the Republic of Kosovo (Boguslaw, 2020, pp. 722, 731). A new surprise came in 2010 when the International Court of Justice

(ICJ) ruled that the Republic of Kosovo had in no way violated international law when it unilaterally declared its independence from Serbia. This ruling drastically changed Serbia's approach to Kosovo's independence (Almqvist, 2013, pp. 181-184; Castan Pinos, 2019, p. 113; Dugard, 2013, pp. 202, 205-206; Escudero Espinosa, 2017, pp. 123-126; Fella, 2024, p. 39; Jelesijević, 2023, p. 30; Newman,Visoka, 2018, p. 374; Nte, 2023, p. 5; Visoka, 2018, pp. 103-104). Thus, the Serbs, with Russian backing, launched a diplomatic counteroffensive to counter Kosovar diplomatic efforts, which had initially succeeded in getting 117 UN member states to recognise their independence. Today, only 90 states still recognise Kosovo's independence, i.e. 46.63% of UN member states. While 78 countries have never recognised it, 13 have withdrawn their recognition of Kosovo's independence, while the position of other countries remains ambiguous (Cakolli, 2020, pp. 15, 19; Castan Pinos, 2019, p. 111; Fella, 2024, p. 37; Jelesijević, 2023, pp. 34-35; Newman,Visoka, 2018, p. 377; Nte, 2023, pp. 1, 9, 13-14; Visoka, 2018, p. 173).

Of the G20 member states, 11 recognise the independence of the Republic of Kosovo (Australia, Canada, France, Germany, Italy, Japan, Saudi Arabia, South Korea, Türkiye, the United Kingdom, and the United States of America), as do 22 of the EU member states (Austria, Belgium, Bulgaria, Croatia, Czechia, Denmark, Estonia, Finland, France, Germany, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Slovenia, and Sweden). The reasons 90 UN member states have declared and maintained their position to recognise Kosovo's independence are less well studied since these specific reasons are often considered less interesting. Several authors identify, however, a number of arguments and reasons that these states may have had when they decided to recognise Kosovo's independence: the violent break-up of the Yugoslav state; the violation of Kosovo's autonomy and human rights by the Milošević-led regime; NATO's military intervention; the Serbs' refusal to negotiate in any way the final status of the province; the favourable decision of the ICJ for the unilateral declaration of independence; the fact that the Republic of Kosovo had undertaken to build a democratic and multi-ethnic state; the support coming from the US and the most prominent EU member states; the uniqueness of the Kosovars' case, which could not easily be repeated; the potential for internationalisation of the territory as a result of ten years of international supervision; the completion of the disintegration of the former Yugoslavia and the achievement of sustainable peace in the Balkan region; the right to self-determination of the majority Albanian population; the lack of international law arguments against unilateral declaration of independence; the diplomatic pressure from the West to recognise Kosovo's

independence. It is also worth mentioning that the maintenance of international presence and supervision over the Republic of Kosovo has been stipulated as a sort of condition for the recognition of independence by some states (Almqvist, 2013, pp. 173-176; Newman, Visoka, 2018, pp. 373-375; Nte, 2023, pp. 11-13). Kosovars promptly complied with this requirement, promising to continue cooperation with the UN and the EU (Dietrich, 2010, p. 127).

Eight G20 member states do not recognise Kosovo's independence (Argentina, Brazil, China, India, Indonesia, Mexico, Russia, and South Africa), as do five EU member states (Cyprus, Greece, Romania, Slovakia, and Spain). The most important reasons why these countries have decided not to recognise the Republic of Kosovo's independence are related to the diplomatic context and national interests. The official justifications most often invoked are respect for Resolution 1244, territorial integrity and sovereignty of states, non-interference in the internal affairs of other states, inter-state equality and peaceful settlement of conflicts (Achcar, 2023, pp. 152-153; Almqvist, 2013, pp. 176-178; Dobrokhotov, 2018, pp. 58-59; Kos-Stanišić, Luša, 2018, pp. 242, 244-246, 250-251; Metodiev, 2018, p. 293; Nte, 2023, pp. 9-11). In reality, however, there are almost always other reasons that weigh more heavily in favour of the decision not to recognise the independence of the Republic of Kosovo, such as concerns about domestic movements towards autonomy or secession. Thus, the protection and promotion of moral, diplomatic, and legal values remain only in the background as more acceptable official explanations for non-recognition (Castan Pinos, 2019, p. 182; Dietrich, 2010, p. 123; Ingimundarson, 2023, p. 196; Kos-Stanišić, Luša, 2018, pp. 242, 252; Metodiev, 2018, p. 293; Newman, Visoka, 2018, pp. 376, 379).

The *"silent countries"* have, however, been almost entirely overlooked by most researchers' analyses despite the large number of states that have decided to refrain from deciding on the Kosovo issue. Even five years after the Republic of Kosovo's unilateral declaration of independence, some 60 states were still in this category, mainly from Africa, Latin America, and Asia. The determining factors for these states' neutrality on Kosovo's independence can only constitute the subject of speculation. It should be emphasised that the terms and conditions of Kosovar secession are a dispute whose resolution is in no way a national stake for many of the world's countries. While the unwillingness of some to take an official position may be explained by the fact that they feel constrained by the dominance and pressure exerted by more powerful countries, others may equally well feel that there are more pressing national issues to be prioritised over diplomacy and foreign

affairs, with recognition of the new states thus somewhere at the bottom of the to-do list. Moreover, supporting one side on such a sensitive issue may raise serious concerns about the grave consequences such a stance could have on relations with the other party involved in the conflict. A final and most legitimate explanation is a well-intentioned concern about clarifying the legality of the unilateral declaration of independence of the Republic of Kosovo under the rules established by international law. No less than 30 such states have asked the UN General Assembly for an advisory opinion from the ICJ on the issue of Kosovo's independence (Almqvist, 2013, p. 178).

Just as in the case of Bosnia and Herzegovina, the recognition of Kosovo's independence was premature, and there are many arguments for this. As is still the case today, the Kosovars did not fully control the territory they proclaimed their sovereignty upon, even in 2008. Northern Kosovo became an enclave that rejected Kosovo's statehood in the February 2012 referendum and is still administered mainly by Serbia, which has set up *"parallel structures"* there, i.e. institutions directly financed and controlled by Belgrade. Thus, a significant consequence of the unilateral declaration of independence is the provocation of a *de facto* ethnic partition of the province, constituting a severe violation of the principles in the name of which NATO intervened in the 1999 campaign (Castan Pinos, 2019, pp. 134-135; Dugard, 2013, p. 207; Džihić, Kramer, 2009, p. 5). Then, the perennial presence of the UN and EU institutions undermines without a doubt any absolute independence of the Republic of Kosovo, which leaves more of the impression that it is, *de facto*, a joint protectorate of the UN, the EU and NATO. Thus, it seems that the states that recognised its independence did so not because they fulfilled the conditions of statehood laid down by the Montevideo Convention but rather to ensure that these conditions would be fulfilled due to the act of recognition of independence. In a world first, dozens of UN member states have recognised the independence of a state that is not at the end of the state-building process but at its very beginning. Moreover, from 1999 until 2008, Kosovars lost their case for independence over Serbia's suppression of autonomy and crimes against humanity. While the declaration of independence immediately after the end of the war might have given them the right to invoke them, by 2008, these arguments had already been lost since the Kosovar province enjoyed a high level of autonomy guaranteed by the UN administration and Serbia itself had already undergone many radical changes, transforming itself into a democratic state where human rights are respected. Furthermore, the roles were reversed in those nine years between the end of the war and the declaration of independence. While the rights of Albanian Kosovars

were protected, the Serb minority in Kosovo became the target of ill-treatment by the Albanian majority (Dugard, 2013, pp. 207-209, 211-212; Jelesijević, 2023, p. 29).

RUSSIA AND THE IMPLICATIONS OF THE KOSOVO PRECEDENT FOR GEORGIA AND UKRAINE

Western states were naïve to think that Kosovo's independence would be accepted as a *sui generis* case that would not serve as a precedent for other movements with secessionist aspirations. The big surprise came, however, when the Russian Federation immediately used the Kosovar precedent to justify its actions in Abkhazia and South Ossetia. On 7 August 2008, Georgia launched a military offensive in South Ossetia, protected by Russian *"peacekeepers"*, although even Russia had recognised the territory as an integral part of Georgia prior to the military campaign. Russia's response was swift, forcing Georgian troops to leave the region after just five days. At the same time, Russian and Abkhaz troops, already occupying most of Abkhazia, forced the Georgian army to withdraw from the Kodori Valley, allowing the Russians and Abkhaz to take control of the whole of Abkhazia. Russia used the Georgian offensive in South Ossetia to justify its actions, forcing Georgia to admit defeat and sign a peace agreement under international auspices. Three weeks into the Georgian campaign, Russia had already recognised the independence of Abkhazia and South Ossetia. As with Kosovo, constitutionally, Abkhazia and South Ossetia were autonomous regions within Georgia, which, after the disintegration of the Soviet Union, sought independence by force with political support from Russia. Both declared independence unilaterally, immediately after the collapse of the Soviet giant, but neither had managed to have their independence recognised by any UN member state, not even Russia, at least until the invasion in 2008. Nevertheless, after the Russian Federation decided, on 26 August 2008, to recognise their independence, several UN member states decided to follow the Russians' lead and recognised the independence of Abkhazia and South Ossetia: Nicaragua, Venezuela, Nauru, Syria, Tuvalu and Vanuatu. The latter two, however, would later withdraw their decision to recognise the independence of the two Georgian regions. Before August 2008, the UNSC had adopted several resolutions reaffirming Georgia's territorial integrity. Although such resolutions could not be adopted after the 2008 war, other organisations immediately condemned the two secessions. The EU, OSCE and NATO reaffirmed their respect for Georgia's territorial integrity in August and September 2008 (Castan Pinos, 2019, pp. 164-165; Dugard, 2013, pp. 212-214; Ingimundarson, 2023, pp. 187-191; Jelesijević, 2023, pp. 31-32,

34; Vakhtangidze, 2011, pp. 402-405; Visoka, 2018, pp. 172, 174, 180). Following Russia's invasion of Ukraine in 2022, South Ossetia expressed its intention to hold a referendum on its integration into the Russian Federation in the summer of the same year. This decision was influenced by the province's failure to demonstrate its viability as a state and North Ossetia's membership of the Russian Federation. Although it dropped this plan for further consultations with the Russian side, South Ossetia's goal of becoming an integral part of Russia has not changed. Abkhazia, the more economically powerful of the two provinces, has shown no such intention and has also rejected any constitutional ties with Georgia. However, Abkhaz citizens remain heavily dependent on the Russian Federation for external representation since Abkhazians without Russian passports are *de facto* stateless (Ingimundarson, 2023, p. 191).

Russia was and still is a particular case in the Kosovar independence equation. A traditional ally of the Serbs, it found itself unable to actively help the latter in the 1999 military conflict, even though it vehemently opposed NATO aggression against Serbia. Nevertheless, Russia remains the Serbs' reliable helper on the issue of Kosovo's independence, with the Russians arguing from the outset that the unilateral declaration violates the norms of international law and does nothing but destabilise the fragile peace in the Balkan region. Its military aggression in Georgia and Ukraine, however, has meant that the intransigence with which the Russian state once rejected Kosovar independence has dissipated both with its recognition of the independence of Abkhazia and South Ossetia (2008) as well as after the recognition of independence and the subsequent official declaration of the annexation of Crimea (2014), Donetsk, Kherson, Luhansk and Zaporizhia (2022) in the name of *"denazification"*, *"demilitarisation"* or *"recovery of Russian territories"*. Thus, the new Russian discourse asserts that the recognition of each declaration of independence constitutes a separate case (Achcar, 2023, pp. 104, 152-156, 174; Baranovsky, 2015, pp. 275-280; Castan Pinos, 2019, pp. 164, 166-167; Dietrich, 2010, p. 130; Dobrokhotov, 2018, p. 57; Ingimundarson, 2023, pp. 185-187, 193-194; Jelesijević, 2023, pp. 29-31, 35; Kos-Stanišić, Luša, 2018, p. 246; Metodiev, 2018, p. 292; Newman, Visoka, 2018, pp. 377, 379; Rotaru, Troncotă, 2017, pp. 328-329; Visoka, 2018, pp. 174, 181-182). It is worth noting that the Kosovo War marked both the first official, straightforward and blunt anti-Western stance of the new Russian Federation and the first occasion on which the Russian population expressed its indignation at the actions of Westerners. From then until now, Westernophobia has almost become Russia's official line in foreign and domestic affairs alike, both ideologically and practically. Today, Russia positions

itself and operates as an adversary and antagonist to Western countries. At the same time, the *"phenomenon of sincere anti-Westernism"* is increasingly present in Russian society, especially after the invasion of Ukraine and the sanctions it brought on the Russian population (Baranovsky, 2015, pp. 275-277; Ingimundarson, 2023, p. 186). If the Kosovar precedent had not existed, it is unlikely that Russia would have invaded Georgia and Ukraine, let alone recognised the independence and even annexed territories internationally recognised as belonging to other UN member states. The Kosovar precedent has done nothing but give the Russians the power of example and the confidence that they can act as they please while positioning them against the Western world (Baranovsky, 2015, pp. 277-280; Castan Pinos, 2019, pp. 164, 166-167; Dugard, 2013, p. 260; Ingimundarson, 2023, pp. 189-190, 193-194; Jelesijević, 2023, p. 30; Rotaru, Troncotă, 2017, p. 332; Vakhtangidze, 2011, pp. 405-406). For Serbia, however, Russia's military actions in Georgia and Ukraine represent potent blows against the arguments it has tried to build around respect for international law. Consequently, Serbs refused to recognise their legitimacy (Džihić, Kramer, 2009, p. 6; Ingimundarson, 2023, p. 196).

Contrary to warnings from Serbia and other countries concerned about the possibility of Kosovo's unilateral independence becoming a dangerous precedent, the world has not seen an explosion of such declarations of independence after 2008. However, various actors in the Balkans and the Caucasus have tried to use the Kosovar precedent, mainly separatist movements, in their efforts to gain international recognition of independence and to consolidate their power over the territories they control or are trying to control, since contemporary international law does not prohibit secession. None, however, proved anywhere near as deft as Russia, a powerful external actor that has explicitly used this precedent to justify its military aggression in Georgia (2008) and Ukraine (2014-present). Equally, where Russia's foreign interests took precedence, namely in Azerbaijan and Moldova, assurances came from the Kremlin that recognising the independence of Abkhazia and South Ossetia would not constitute any precedent for facilitating the recognition of the independence of the Republic of Artsakh and the Pridnestrovian Moldavian Republic. In 2023, however, Russia withdrew its recognition of Moldova's sovereignty over the latter, leading to fears that annexation could follow once Russia recognises the Pridnestrovian Moldavian Republic's independence. Looking again towards the Balkan Peninsula, the political class in Republika Srpska, one of the three administrative entities recognised by the Bosnian state, has also tried unsuccessfully to use the Kosovar precedent in an attempt to leave Bosnia and Herzegovina. There are also fears that the sizeable Albanian minority in North Macedonia could

also follow the path of its Kosovar brothers, given the violent episodes that have continued inter-ethnic tensions even after the end of the 2001 war. However, it remains complicated to predict the medium- and long-term consequences of the Kosovars' declaration of independence (Castan Pinos, 2019, pp. 158-161; 164-169, 182; Dietrich, 2010, p. 130; Džihić, Kramer, 2009, p. 5; Escudero Espinosa, 2017, p. 107; Hrnjaz, 2020, p. 397; Ingimundarson, 2023, pp. 187, 192-195; Jelesijević, 2023, pp. 29-30; Richter, Halbach, 2009, pp. 228-232, 237).

The Kosovo – Republika Srpska parallel revealed a severe legal double standard when the ICJ cited UNSC Resolution 787 as an example of the UNSC condemning certain unilateral declarations of independence. The ICJ's failure to identify any prohibition in international law preventing a unilateral declaration of independence by the Republic of Kosovo directly conflicts with Resolution 787 since both the Republic of Kosovo and Republika Srpska were ethnic minority enclaves within federal states of former Socialist Federal Republic of Yugoslavia. If today there is no prohibition in international law on the secession of the Republic of Kosovo, whose majority Albanian population constituted a minority within the former federal state of Serbia, then neither can the unilateral declaration of independence of the Republika Srpska, whose majority Serb population constituted a minority within the former federal state of Bosnia and Herzegovina, be categorised as in any way violating international law (Dugard, 2013, pp. 168-170). As far as North Macedonia is concerned, the Western stance towards the Albanian insurgency in this former Yugoslav state reveals an apparent double standard concerning the actions they have taken about the Kosovo conflict. While the Albanian rebels in the province of Serbia received the full support of the West, the Albanian rebellion in North Macedonia was universally condemned, even though it was encouraged by the very actions of the West in the Balkans, particularly in the province of Kosovo. The same international actors that supported by all possible means the Albanian insurgency in Kosovo in 1999 labelled the Albanian insurgents in North Macedonia as terrorists just two years later. This shift in the official discourse is all the more astounding if we take into account that many of the Albanian militants in North Macedonia had previously fought in Kosovo with the KLA (Castan Pinos, 2019, p. 161).

Kosovo – Ukraine is, however, still the most notable parallel in terms of the blatant double standard we find in both the discourse and the actions of some Western states. Although they accepted, justified and supported the violation of the territorial integrity of Yugoslavia, ignoring the UNSC and international law in favour of geopolitics and the manifestation of power, the same states declared themselves to be outraged by similar actions taken by Russia in Georgia and especially in Ukraine,

the consequences that the Russian state had to face for violating the sovereignty of these states being among the most severe (Achcar, 2023, pp. 168-169; Castan Pinos, 2019, p. 178; Hrnjaz, 2020, pp. 397-398; Jelesijević, 2023, pp. 29-31; Rotaru, Troncotă, 2017, pp. 326, 328-329, 336; Vakhtangidze, 2011, p. 407). The exact parallel also tells us of the double standard applied by the Kremlin on secessionism, as the official discourse of the Russian Federation on this issue reversed in the 15 years from the end of the Kosovo War to the annexation of Crimea. When the province unilaterally declared its independence in 2014, the Russians enthusiastically supported it, describing it as a *"manifestation of the right of peoples to self-determination".* Nor did Kyiv's lack of agreement bother Russia nearly as much as Belgrade's lack of agreement did when the Republic of Kosovo unilaterally declared its independence, which the Kremlin criticised so severely. Moreover, if, in the case of Kosovo, they vehemently opposed any external intervention, the Russians found it imperative in Crimea to use external force in the name of prevention *"so as not to wait until it would already be too late"* (Baranovsky, 2015, p. 278; Castan Pinos, 2019, pp. 166-167; Ingimundarson, 2023, p. 186; Jelesijević, 2023, pp. 29-31). Therefore, both Westerners and Russians apply double standards when it comes to secessionist movements and the recognition of their independence. On the one hand, when Kosovars declared their independence, Russia invoked the strict preservation of Serbia's territorial integrity, a principle of international law that it abandoned shortly afterwards when it supported the secession and independence of Abkhazia and South Ossetia, the Russians' arguments being the same ones that Westerners used to justify their support for Kosovo's independence. On the other hand, the Westerners came to Georgia's defence, invoking the principle of respect for territorial integrity, the same principle they refused to respect when they violated Serbia's sovereignty (Castan Pinos, 2019, pp. 166-167; Džihić, Kramer, 2009, pp. 6-7; Jelesijević, 2023, pp. 29-31).

Equally, in 1991, when the Chechens unilaterally declared their independence from the Russian Federation following the disintegration of the Soviet Union, the international community condemned Russia's violation of territorial integrity just as strongly, even though the same Western states fervently supported or even participated in the violation of Serbia's territorial integrity by the Kosovars. Therefore, if the ICJ has determined that Kosovo's unilateral declaration of independence in no way violates international law, then the Chechens would not violate it if they declared independence again today (Dugard, 2013, pp. 174-176; Ingimundarson, 2023, p. 196). A parallel can also be drawn between Kosovo, Abkhazia and South Ossetia. Just as in the case of the Western powers with the Republic of Kosovo, Russia

decided on a premature recognition of the independence of these two Georgian regions, even though South Ossetia did not fully control the territory over which it had proclaimed its sovereignty, while Abkhazia's policies and structures were still mainly under the control of the Kremlin, especially in terms of defence and security institutions, reminiscent of the Western protectorate over the Republic of Kosovo. Nor could the two Georgian regions claim that their right to autonomy had been violated or that the Georgians had committed crimes against humanity on their territory. On the contrary, in the 1990s, the Abkhazians were responsible for the expulsion of Georgians from the region. However, this process of ethnic cleansing was not caused by any human rights violations by the Georgian majority. Moreover, applying the same tactics that the Kosovars used, it was the Ossetians who initiated the military clashes, provoking Georgia's reaction to launch a military offensive in South Ossetia, which provided the Russians with the ideal pretext for intervention (Dugard, 2013, pp. 215-218; Ingimundarson, 2023, pp. 190-191; Vakhtangidze, 2011, p. 413). Taking all these aspects into account, the actual Russian position on secessions can be summarised as follows: if secession affects Russian territory, as was the case with Chechnya, then it is unacceptable; if there are specific interests at stake, it can be used as a bargaining tool, as was the case with the Kosovar province; if strategic partners suffer because of political instability or military conflict, it can be used to their advantage, as was the case in the post-Soviet space; and, of course, if it results in territorial gains for the Russian Federation, then secession is perfectly acceptable (Baranovsky, 2015, p. 279).

CONCLUSIONS

The final status of the Albanian community in the province of Kosovo, which they wish to transform into a new state, has not been resolved by the policies related to recognising the unilateral declaration of independence of the Republic of Kosovo. In the absence of guarantees and certainty that recognition of statehood can be achieved at some point in the future, these policies are marked by a strong incongruity with the notion of a standardised procedure. The political struggle can only end when statehood is achieved beyond doubt, but this *status quo* may remain only a chimaera. Indeed, it will still be in the political sphere where the fierce negotiations on the recognition of the independence of the Republic of Kosovo and any other new entities that unilaterally aspire to statehood will continue. Even though, in an ideal world, strong arguments should be the decisive factors in shaping an outcome accepted by both sides at the end of these negotiations, the reality of international affairs has repeatedly shown us that lobbying and pressure

from powerful states determine the direction of the negotiations, which does not always lead to a final result (Almqvist, 2013, p. 186). Consequently, despite the high number of UN member states recognising Kosovo's independence, Kosovo can become a member of the organisation only with Serbia's consent and only if Russia and China stop using their veto. Equally, the chances of survival of unilaterally declared states with Russia's backing at the expense of Georgia and Ukraine are difficult to predict (Dugard, 2013, pp. 201-202).

The analysis of the politics of recognising the independence of the Republic of Kosovo revealed that, on the one hand, the motives for supporting Kosovo's independence are mainly common to most of the states that have supported and maintained their recognition of the Kosovars' state: the portrayal of Kosovars as martyrs of Serbian cruelty, support for the human rights and aspirations of the Albanian majority, and the inescapable influence of both the major European powers and the USA. On the other hand, the facts of the non-recognition of Kosovo's unilateral declaration of independence are much more complex. Although the official motivation of the states that have taken this diplomatic stance towards the independence of the Kosovars falls, at least at a declaratory level, within the sphere of respect for UN decisions, the territorial integrity of states, and the principles of non-interventionism, peaceful resolution of conflicts and support for international law, the geopolitical realities are more likely to indicate that internal factors prevail, since almost every one of these states is also facing problems caused by various movements seeking autonomy or even secessionist objectives.

Although it has historically been both a strong ally of Serbian interests and rights in international politics, often demonstrating implacable and seemingly disinterested support for Serbia's cause, thus being the most crucial ally the Serbian state has had against Kosovar separatists, these considerations did not prevent Russia from tempering its rhetoric against recognising the independence of the Republic of Kosovo when national interests demanded it, cleverly using the Kosovar precedent to justify its separatist gains and aspirations in Georgia and Ukraine to annex the territories mentioned above. Russia used the West's support for Kosovo's independence as a pretext to instrumentalise the contested international norms to further its geopolitical and territorial aspirations. In order to achieve its foreign policy objectives in Georgia and Ukraine, Russia has sought, on the one hand, to exert its authority and power over the spheres of influence it claims by using euphemisms such as *"post-Soviet space", "near neighbourhood"* or *"regions of privileged Russian interest"* and, on the other hand, to compete geopolitically with the West either by imitation or by categorising its actions as mere replication of those attributed

to the West (Ingimundarson, 2023, p. 186). Therefore, the policies of recognising Kosovo's independence depend on the national interests of each state. It is demonstrated unequivocally by the fact that each of the 13 G20 and EU member states that do not recognise the Kosovars' right to independence have either recently had to deal with or are still dealing with various notable movements with autonomist or secessionist aspirations.

To sum it all up, despite the frequent warnings from UN representatives who intransigently express that the organisation's position is that the Republic of Kosovo is a particular case that should not be adopted as a benchmark by other separatist movements (Dietrich, 2010, p. 130), the unilateral declaration of independence of the Republic of Kosovo has lost its *sui generis* status, since, *de facto*, the Kosovar precedent significantly influences international politics by providing a model for secessionist movements everywhere to follow, the Kosovar path to independence becoming for them a kind of guide whose steps must be followed in order to achieve their separatist goals. Thus, in order to gain international sympathy and credibility, secessionist movements need to demonstrate not only that there is some form of discrimination in the country of which they are part but also that there are a significant number of atrocities committed against their members, who are usually a minority at the national level. However, if governments do not commit such acts against them, members of separatist movements will provoke them to achieve their aims. Once these steps have been taken, all that is left for the representatives of these movements to do is to attract as many international actors as possible to their side, and this often proves to be the most challenging step of all. Of course, national governments are also aware of these steps. They will try to demonstrate that they democratically represent the entire population of their country without committing any inhumane or discriminatory acts. Less powerful states will try to attract international support, justifying their cause as *"fighting terrorism".* In the end, the final status of the community aspiring for independence and the territorial integrity of the state in question is decided by who manages to win this diplomatic war between the secessionist movement and the national government (Hrnjaz, 2020, pp. 399-400).

BIBLIOGRAPHY:

1. Achcar, G. (2023). *The New Cold War: The United States, Russia, and China from Kosovo to Ukraine*. Chicago: Haymarket Books.
2. Almqvist, J. (2013). *The politics of recognition: The question about the final status of Kosovo.* In D. French (Ed.), *Statehood and Self-Determination: Reconciling Tradition and Modernity in International Law* (pp. 165-186). Cambridge: Cambridge University Press.

3. Baranovsky, V. (2015). *From Kosovo to Crimea*. In *The International Spectator*, 50(4), pp. 275-281. doi:10.1080/03932729.2015.1092677.
4. Boguslaw, A. (2020). *Suddenly Everyone Started to Love Our Anthem, Our Flag: Identity Construction, Crisis, and Change,* in (Almost) Sovereign Kosovo. *Nationalities Papers,* 48(4), pp. 721-736. doi:10.1017/nps.2018.78.
5. Cakolli, E. (2020). *Kosovo: Between universal non-recognition and 'derecognitions'*. Pristina: Kosova Democratic Institute.
6. Castan Pinos, J. (2019). *Kosovo and the Collateral Effects of Humanitarian Intervention*. Abingdon: Routledge.
7. Centanni, E. (2020), *Political Geography Now*, https://www.polgeonow.com/2020/09/which-countries-recognize-kosovo-independence.html, retrieved on 22 May 2024.
8. Chomsky, N., Džalto, D., Grubačić, A. (2018). *Yugoslavia: Peace, War, and Dissolution*. Oakland, CA: PM Press.
9. Montevideo Convention (1933). *Montevideo Convention on the Rights and Duties of States*. Montevideo: The 7th International Conference of American States.
10. Cox, J.K. (2002). *The History of Serbia*. Westport, CT: Greenwood Publishing Group.
11. Kosovo Declaration of Independence (2008). *Kosovo Declaration of Independence*. Pristina: Kosovo Parliament.
12. Dietrich, F. (2010). *The status of Kosovo – reflections on the legitimacy of secession*. *Ethics & Global Politics,* 3(2), 123-142. doi:10.3402/egp.v3i2.1983.
13. Dobrokhotov, L.N. (2018). *Kosovo as a Factor of the World Order Change*. In D. Proroković (Ed.), *Kosovo: Sui Generis or Precedent in International Relations* (pp. 54-65). Belgrade: Institut za međunarodnu politiku i privredu.
14. Dugard, J. (2013). *The Secession of States and Their Recognition in the Wake of Kosovo*. Hague: Hague Academy of International Law.
15. Džihić, V., Kramer, H. (2009). *Kosovo After Independence: Is the EU's EULEX Mission Delivering on its Promises?* Berlin: Friedrich-Ebert-Stiftung.
16. Escudero Espinosa, J.F. (2017). *Self-Determination and Humanitarian Secession in International Law of a Globalized World: Kosovo v. Crimea*. Cham, Switzerland: Springer.
17. Fella, S. (2024). *Kosovo: developments since 1999 and relations with Serbia*. London: House of Commons Library.
18. Hrnjaz, M. (2020). *Twenty years after the NATO armed intervention: The Kosovo case and remedial secession*. *Međunarodni problemi*, 72(2), pp. 379-403. doi:10.2298/MEDJP2002379H.
19. Ilic, L. (2013). Wikimedia Commons, https://commons.wikimedia.org/wiki/File:Map_of_ethnic_groups_in_Kosovo,_2011_census.gif, retrieved on 22 May 2024.
20. Ingimundarson, V. (2023). *Russia's Use of the Kosovo Case to Legitimize Military Interventions and Territorial Conquests*. In R.Z. Aliber, M. Gudmundsson, G. Zoega (Eds.), *Fault Lines After COVID-19: Global Economic Challenges and Opportunities* (pp. 185-198). Cham, Switzerland: Palgrave Macmillan.
21. Jelesijević, A. (2023). *The Application of Remedial Secession in the International Law* (Case Study: Kosovo, Abkhazia, South Ossetia and Crimea). *Ukrainian Policymaker,* 12(3), pp. 28-37. doi:10.29202/up/12/3.

22. Kos-Stanišić, L., Luša, Đ. (2018). *Position of Latin America towards Kosovo*. In D. Proroković (Ed.), *Kosovo: Sui Generis or Precedent in International Relations* (pp. 239-259). Belgrade: Institut za međunarodnu politiku i privredu.
23. Metodiev, K. (2018). *Catalonia and Kosovo Cases (Comparative Analysis)*. In D. Proroković (Ed.), *Kosovo: Sui Generis or Precedent in International Relations* (pp. 273-298). Belgrade: Institut za međunarodnu politiku i privredu.
24. Newman, E., Visoka, G. (2018). *The Foreign Policy of State Recognition: Kosovo's Diplomatic Strategy to Join International Society*. In *Foreign Policy Analysis,* 14(3), 367-387. doi:10.1093/fpa/orw042.
25. Nte, T.U. (2023). *The Burden of Recognition in the Unilateral Declaration of Independence by Kosovo*. In *Global Journal of Political Science and Administration,* 11(1), 1-19. doi:10.37745/gjpsa.2013/vol11n1119.
26. Richter, S., Halbach, U. (2009). *A dangerous precedent? The political implications of Kosovo's independence on ethnic conflicts in South-Eastern Europe and the CIS. Security and Human Rights,* 20(3), pp. 223-237. doi:10.1163/187502309789192496.
27. Rotaru, V., Troncotă, M. (2017). *Continuity and change in instrumentalizing 'The Precedent'. How Russia uses Kosovo to legitimize the annexation of Crimea. Southeast European and Black Sea Studies,* 17(3), pp. 325-345. doi:10.1080/14683857.2017.1348044.
28. UNSCR 1244 (1999). *Resolution 1244*. New York City: UN Security Council.
29. Vakhtangidze, V. (2011). *The Impact of Kosovo: A Precedent for Secession in Georgia?* In J. Summers (Ed.), *Kosovo: A Precedent? The Declaration of Independence, the Advisory Opinion and Implications for Statehood, Self-Determination and Minority Rights* (pp. 395-426). Leiden: Martinus Nijhoff Publishers.
30. Visoka, G. (2018). *Acting Like a State: Kosovo and the Everyday Making of Statehood*. Abingdon: Routledge.
31. 38 I.L.M. 1217 (1999), *Military Technical Agreement between the International Security Force ("KFOR") and the Governments of the Federal Republic of Yugoslavia and the Republic of Serbia*, Kumanovo.

TÜRKIYE
– NAVIGATING ROLES AS AN UNCOMFORTABLE ACTOR OR REGIONAL "BALANCER" –

Assistant Professor Oana-Elena BRÂNDA, PhD
"Titu Maiorescu" University, Bucharest
DOI: 10.55535/RMT.2024.4.31

This article aims to explore two roles assumed by Türkiye in the international environment: the one of uncomfortable state actor for the West and the neighbourhood, even problematic at times, and the one of regional "balancer", interested in identifying the appropriate course of action to end the war of Russia against Ukraine. Capitalising on its imperial heritage as well as its geographical location, Türkiye has over time had a number of strengths which it has exploited in its international relations to achieve its interests. The year 2023 brought with it the reconfirmation of a new mandate of President Erdogan, aspect seen as decisive in the configuration of the mentioned image – of an inconvenient actor – of Türkiye. However, this Türkiye, considered by many to be inconvenient, has remained extremely consistent in its relation to the Russian-Ukrainian war, manifesting itself as a "balancer" by attempting to create favourable premises for its conclusion.

Keywords: balance of power; war; political system; international relations; regional power;

INTRODUCTION

Throughout history, Türkiye presented itself as an interesting actor, even an intriguing one, as a result of its decisions on both domestic and foreign affairs. This posture is owed to the fact that, in some cases, the country seemed to head towards the West, while in others, it was accused of paying lip service to Russia.

Ever since the Russian war of aggression against Ukraine broke out, Türkiye was extremely active as far as ending the war is concerned, both by vocally and pragmatically advocating in favour of the Ukrainian integrity and sovereignty, as well as through the military support provided to Ukraine. Despite the fact that Türkiye seems to have a *"special relationship"* with Russia – a fact that resulted from the bilateral relations in terms of foreign policy, its support to Ukraine saw no step back.

The present article explores a current issue and question at the same time – *Is Türkiye an uncomfortable actor or rather a significant regional "balancer"*? In order to provide an answer, the article shall undergo a review of recent political events within the country, their reflection on the domestic level, followed by the analysis of foreign intended actions, meant to restore the state's reflection on an international level. In order to illustrate these evolutions, and to prevent this article from becoming a book chapter (given the impressive academic analysis existent on the topic), the attention shall be focused on the result of the 2023 Turkish Presidential elections, followed by Türkiye's attempt to mediate the negotiations that would put an end to the Russian war against Ukraine. Although there is no evident causality relationship between the two, they remain important to illustrate and justify the current Turkish standing within the Black Sea area.

MAIN EVOLUTIONS IN THE FUNCTIONING OF THE CURRENT TURKISH POLITICAL SYSTEM

2023 was an important year for Türkiye, as a result of the stakes riding on it. The February earthquake was an alarm call on the state's capacity to deal with crises of such magnitude. Moreover, government popularity was down as a result of economic difficulties – in 2022, inflation rates hit 72.3% (Focus Economics, 2022). As a result, given the fact that presidential elections were scheduled to be held in May 2023, the international public opinion was tuned to those evolutions. The main question was whether the elections would bring along political change,

or the Justice and Development Party (AKP) – the party of the current president – would remain in power.

Currently, the question has been answered: on 3 May 2023, Recep Tayyip Erdogan entered his third mandate as President of Türkiye. Furthermore, the May 2023 elections did not only reconfirm Erdogan as president, but were also a reflection of a series of evolutions since 2016 onwards, many of them highly criticised by the international community. The most important of these evolutions shall be explained below.

The attempted Turkish coup d'etat of July 2016 resulted in the creation, on the level of the Turkish leadership, of an alarming perspective with regard to internal and external enemies. Thus, as a result of the July 2016 action, the Turkish government established a state of emergency within the state, which led to a restraint of the freedoms set by the Constitution. At the time, approximately 40,000 government workers were laid off, then arrested, and several educational facilities, associated with Fethullah Gulen (the exiled Islamist leader who orchestrated the coup d'etat) were shut down (Human Rights Watch, 2016).

The April 2017 referendum led to the changing of the political system, from a parliamentary republic (dating back to 1923) to a presidential one (based on the US model). In January 2018, the very legislation that provided the President with unlimited powers and removed the Prime Minister position, was enacted.

Although the Turkish political system has always been an etatism-based one, the new Constitution allows the President to leave aside the Parliament in the exercise of its ruling function. Consequently, the main critique verbalised internationally on the Turkish political system is that democracy is not inclusive and serious violations of human rights are likely to occur.

At present, the ruling of Erdogan is a projection of force, which is likely to impose costs on the Turkish state, since more and more international organizations in the field of human rights protection began signalling deviations within the Turkish political system. Thus, in 2017, the Council of Europe Parliamentary Assembly launched a monitoring procedure on Türkiye, invoking its concern on the violations of human rights, democracy and rule of law (Council of Europe, 2017). In 2018, the UN Office for Human Rights issued an evaluation report on the state of human rights post-coup d'etat in Türkiye. The assessed time frame ranged between 1 January – 31 December 2017, and the results were concerning, given the fact that in the context of the state of emergency established immediately after the coup d'etat, arbitrary denial of freedom of movement as well as that on the right to work occurred. Claims state that they were followed by torture and bad treatments,

and the violation of the right of association and freedom of speech. For instance, in the case of the arrests performed as a result of the coup d'etat, detention was accompanied by torture, loss of jobs and social rights, including evacuation from state-owned housing. Furthermore, the violation of freedom of speech occurred in the shutting down of approximately 100,000 Internet sites and TV channels, some of which were accused of being pro-Kurdish (United Nations, 2018). In addition, the report pointed out that the changes in the 2017 Constitution affected justice impartiality and limited Parliamentary control over the Executive.

In 2021, the Council of Europe, the EU and the USA criticised Türkiye for its withdrawal from the Istanbul Convention on the prevention and combatting of violence against women and domestic violence. Later on, in March 2023, the Council of Europe Ministerial Council reiterated its call for the freeing of the former co-president of the People's Democratic Party (HDP), Selahattin Demirtaş, and of activist Osman Kavala, as a result of the in-favour ruling of the European Court of Human Rights.

As far as his relationship with the Kurdish minority is concerned, in the first years of his mandate, President Erdogan showed concession towards them, by providing cultural rights. However, the military operations in the south of Türkiye led to various deaths, disappearances and torture practices among the Kurds (United Nations, 2018). In addition, after the coup d'etat, the political leaders of the Kurdish movement were arrested, accused of treason and several attempts to discard the People's Democratic Party occurred. Moreover, President Erdogan justified his refusal to Sweden's accession to NATO based on the allegations that Sweden was protecting Kurdish terrorists.

In the spring of 2023, Erdogan's main campaign topics featured national security, an increase in public investments and the preservation of conservatory family values, versus the opposition candidate, Kemal Kılıçdaroğlu, accused of promoting the LGBT community values, against the family-related ones. It is in this framework that an election monitoring mission, jointly performed by the OSCE and the Council of Europe Parliamentary Assembly, highlighted the national and private media biased actions (at the same time, those media channels criticising Erdogan's leadership were systematically fined), the use of public resources in favour of the ruling party, restrictions on the freedom of speech, including arrests and trials of those journalists *"unfriendly to the ruling power"* (Fella, Walker, 2023).

It is obvious, based on the international reports and monitoring missions, that the current Turkish political system is characterised by the concentration of power

in the hands of the president, and the restraint of human rights and freedoms in order to exert a firm domestic control. It is a fact that this domestic conduct has been repeatedly criticised by the international fora.

TÜRKIYE AS AN "UNCOMFORTABLE PARTNER"

Under Erdogan's presidency, Türkiye developed a more assertive foreign policy, featuring its direct military involvement in the Syrian civil war, the performance of military operations in northern Iraq to capture the members of the Kurdistan Workers' Party (PKK), the support for Azerbaijan in its dispute with Armenia for Nagorno-Karabakh, its involvement in the Russian war of aggression against Ukraine and its interventions in the disputes in the Aegean and Eastern Mediterranean seas.

The relations between Türkiye and Syria have been tense ever since 1939, when the former annexed the Hatay province. Other disputes ensued, focusing on the access to water resources of the two states sharing a considerable border, the support offered by Syria to PKK and to the Secret Freedom Army of Armenia (dissolved in the meantime), which the EU and NATO considered to be a terrorist organization. The relations between the two states had their relaxed moments, but once the Syrian civil war broke out in 2011, the diplomatic relations between the two have been severed, to be temporarily re-established in October 2021. Moreover, the results of the Turkish elections have been much coveted, as the Erdogan regime promoted a relaxation in its relations with the Bashar Al-Assad regime (Khalife, Waters, 2023). It was done in order to regulate the situation of Northern Syria, where Türkiye has been stationing military troops, and that of the approximately 3 million Syrian refugees on Turkish ground.

As was the case in Syria, Türkiye has been stationing military troops in Northern Iraq since 1995-1997, in order to capture PKK members. While initially, Iraq expressed its agreement for Türkiye to perform military operations on its territory against PKK members, beginning with 2017 onwards, the Iraqi government protested repeatedly against Turkish military incursions on its territory, claiming it to be a violation of its sovereignty and territorial integrity.

The relationship between Türkiye and Azerbaijan is essential to both, since the latter is an alternative provider to Russian gas, while the former is a well-developed source of weapons to Azerbaijan in its fight against the Armenians in Nagorno-Karabakh.

Ever since the debut of the Russian war of aggression in Ukraine, Türkiye attempted to place itself as a peace-maker, since Ukraine is a zone of interest to Türkiye in its attempt to avoid Russian gas and nuclear dependence. This is highly

important as far as energy costs are concerned, even though, at present, Rosatom plays the lead role in building Türkiye's first nuclear power plant in Akkuyu. Furthermore, even though Türkiye joined NATO member states in condemning the Russian invasion in Ukraine and provided the latter with military equipment, it did not impose any sanctions to Russia and even facilitated the access of Russian businessmen on its territory. At present, Istanbul is a transportation hub for flights to and from Russia. Moreover, in July 2022, Türkiye took on the mediation role, facilitating the *Black Sea Grain Initiative* (*BSGI*).

The conclusion of BSGI provided Russia with access to the Bosphorus for the first time in history, but rather in a controlled manner, as Türkiye ably limited the access of Russian military vessels to the Straits. In light of this access and control within the Black Sea, Russia was deeply interested in the outcome of the Turkish elections. Even though Erdogan considers Putin to be *"a dear friend"* (The Economist, 2022), the Ankara leader is very shrewd in playing his cards – he tempts the West to annoyance, but not badly enough to turn it into an enemy.

Another area of interest to Türkiye is the Eastern Mediterranean, on account of its conflicts with Greece and Cyprus for marine foraging rights, in light of the energy development potential of the area. The relationship between Türkiye and Greece has been a problematic one for decades, and can be summarised in a few words: for the Greeks, Türkiye is a threat, while Türkiye perceives Greece to be an enemy (Coşkun, Ülgen, 2022). The two perspectives are justified by the sovereignty disputes in the Aegean Sea, and by the status of the Turkish minority in Western Thracia. As far as Northern Cyprus is concerned, Erdogan sided with the current political leaders, who rejected the UN solution of a united federal Cyprus, in favour of the two-state solution (Ib.).

From the point of view of the Islamic world, Türkiye is a strategic actor, having particular connections with the European Union and NATO. For Türkiye, NATO is a provider of security guarantees, while the EU is the greatest market for Turkish products. In addition, Türkiye is the main migration route from the east to the centre of Europe. In the Western Balkans, Türkiye is a competitor for Russia and the EU (Haas, 2023). For instance, in Bosnia, Kosovo and Montenegro, Türkiye exerts a manifest patronage over the Turkish minority.

Therefore, why is Türkiye considered to be an *"uncomfortable partner"* for the West and its neighbourhood? The explanation stems from the fact that any Turkish policy, including the foreign one, is based on nationalism, bearing thus significant implications for neighbouring or partner states. For instance, although a member

of NATO and a candidate to the European Union, Türkiye distanced itself from the Euro-Atlantic perspective in the Black Sea region, rejecting the internationalization process and promoting its exclusively regional role, mainly on economic grounds. Furthermore, although its political relations with Syria and Iraq are tense, as presented above, the Turkish MFA would like to retain its two pillars in the East – in Baghdad and Damascus, as any withdrawal from Syria and Iraq would be translated in renouncing its fight with the PKK.

TURKIYE'S *"BALANCER"* ROLE, BETWEEN THEORY AND PRACTICE

The concept of *"balance of power"* is extremely important in the field of International Relations. In a multipolar world, bearing in mind the memory of the Cold War bipolarity, the maintenance of a balance of power remains the aim of international leaders in order to maintain peace, or, should peace be compromised, in order to attain it.

IR theory often makes the difference between *"balancing"* as a type of state behaviour and *"the balance"* as a result from the perspective of foreign policy. Thus, the very essence of *balancing* is meant to develop a state's capacity to resort to military operations in order to discourage or defeat another state. State *balancing* could occur in multiple ways, either by coalescing other states' resources by alliance forging (*external balancing*), or by improving its own military abilities (*internal balancing*). On the other hand, *"the balance"* is used to describe a systemic result – the very balance of military capabilities within the international system. It is important to acknowledge that, although often operated as a distribution of resources among two or more states, the main point of interest of the concept is its ability to prevail in a military conflict (Vasquez, Elman, 2012, p. 30).

Kenneth Waltz (2006, pp. 30-45) differentiates between two types of *balancing*: an internal one, when a state relies on its own efforts, and an external one, when a state forges alliances with other states. Within bipolar systems, on the one hand, *balancing* would occur between the two superpowers, that are likely to fundament their strength on their own efforts and resources and are not likely to appreciate alliances with small states. Contrary to expectations, Waltz claims that the *balance of power*, although being a protection mechanism for the state in order to survive, does not always lead to the absence of war. On the other hand, in a multipolar system, *external balancing* spans two dynamics. Since more than one state is in the capacity to deal with a competitor, each has enough reason to *"pass on responsibility"*, hoping that another threatened state will use its human

and material resources in order to stop a hegemonic power from ascending to more. The passing on of responsibility from one hegemon to another might lead to the absence of any *balancing*. Consequently, one or more of the other states might hold hegemony at a given time.

According to Christensen and Snyder, states are more likely to pass on responsibility, when they consider that the advantage resides with the defensive (1990, pp. 137-168). It means that they will not react and will wait instead for another threatened state to act. In contrast, when states consider the advantage of being on the offensive side, their response will be an active one, likely to lead to a rapid expansion of the war. Thus, Christiansen and Snyder agree with Waltz that the *balance of power* does not automatically translate in the absence of war. Should the offensive be considered a dominant one, states will rush towards forging foreign alliances and towards fulfilling their commitments within. Should defence be considered dominant, the passing on of responsibility will be widespread, while *balancing* will be rare. In a world truly dominated by the offensive, it is probable for potential hegemons to rapidly climb the hierarchic system, and leave no room for balances to occur. The two authors illustrate this idea with the example of the pre-world war alliances. The failure of alliances throughout time to prevent war from occurring shows that *balancing* was not efficient. However, most states will act in order to counter a possible hegemon. In addition, they would comprehend the probability of a systemic result in need to be avoided (another state hegemony), and would act to achieve the preferred systemic result (the very balance).

Even though the *balance of power* was consecrated in the field of International Relations and was operated by states to maintain equilibrium within the international community, its achievement requires a series of attributes such as: wisdom, initiative, perseverance and diplomatic creativity.

From the point of view of Ahmet Davutoglu, President Erdogan's foreign affairs counsellor, who, in 2016, became Minister of Foreign Affairs in the administration of the same president, Türkiye's current standing, as a successor of the former Ottoman Empire, places it, both geographically and politically, in the *"balancer"* spot. Based on its succession of the Ottoman Empire and on its spheres of influence, Türkiye belongs to the Middle East, the Balkans, the Caucasus, Central Asia, the Caspian Sea, the Mediterranean and the Black Sea (Sanchez-Tapia, 2022). It is based on this perspective and on its geographical positioning in Eastern Europe, that Türkiye assumed the *"balancer"* role in the Russian war of aggression against Ukraine, which started on 24 February 2022.

The *"balancer"* role took on by Türkiye ever since the beginning of the war, although initially considered to be risky, was, in fact, the winning strategy. Thus, Türkiye managed to support Ukraine, both politically and militarily, without alienating Russia from an economic point of view.

There are several actions that Türkiye pursued since the beginning of the Russian war against Ukraine, which feature it as a veritable *"balancer"*: its refusal to acknowledge the illegal annexation of Crimea and its insistence for the maintenance of Crimea's territorial integrity within its 1991 borders. Moreover, Türkiye was the first country to provide Ukraine with drones, at a time when other states were still debating on the kind of military support to be provided to Ukraine. Within the same line of action, the Turkish decision to close down the Bosphorus and Dardanelle straits for Russian war ships prevented the escalation of the fight in the Black Sea.

Other diplomatic actions, better focused on ensuring the *balance of power* consist of: the facilitation of a meeting between Dmytro Kuleba, the Ukrainian foreign minister and Sergey Lavrov, the Russian one, in the format of the Antalya Diplomatic Forum of 10 March 2022, as well as the facilitation of negotiations at the end of March 2022, in Istanbul, in order to help identify a solution that would lead to the end of the war.

A resounding, yet temporary success of Türkiye's *balancing* act resides in the signing of the grain agreement. Türkiye capitalized on the signing of the agreement in order to advance on the establishment of the Istanbul Common Coordination Centre that would help the implementation of the BSGI, as a means to increase the confidence between Russia and Ukraine, and thus end the war.

The BSGI is an accomplishment of Türkiye's mediation efforts, but the implementation of the Initiative need not be regarded only in commercial terms – that of ensuring the export of Ukrainian grains, but also in humanitarian terms, as was put in the words of Turkish officials (Sofuoglu, 2022), to contribute to the softening of the food crisis on a global level. Although the BSGI rode on high stakes – as Turkish foreign affairs minister, Mehmet Cavusoglu mentioned that, once the implementation of the BSGI became effective, the next step would lead to the consolidation of a certain form of trust between Russia and Ukraine that would lead to the ending of the war (Aydogan, 2022) – the results were not the intended ones. What is more, Russia bombed Odessa the following day after the signing of the agreement, and unilaterally withdrew from it in July 2023.

As the war in Ukraine progressed, Türkiye's *balancer* stand was confronted with criticism in international discourse. It was claimed to be guilty of its intensification of economic relations with Russian companies, allowing Russian businessmen

to escape international sanctions, while allowing Russia to use Turkish ports in order to sell the grains abusively collected from Ukraine (Gaber, 2022).

By supporting Ukraine, Türkiye enhanced its stronghold within the region, at the same time as exposing itself to risks. The greatest one emanated from Russia, which continues to be a threat in Syria, where its presence can destabilize the border and lead to new waves of immigrants (Ib.). Türkiye is also dependent on the Russian imports of energy. Yet, the relationship between the two is ampler. Despite the fact that Russia is a threat to NATO, the close relationship that President Erdogan and President Putin share, turned Türkiye (a NATO member state) into a shelter for Russian citizens and businessmen.

Despite the actions of Turkish decision-makers and the diplomatic agreements brokered by Türkiye – the grain agreement and the exchange of prisoners between Russia and Ukraine at the beginning of 2023 are considered to be successes of the Turkish diplomacy *balancing* act, and despite President Erdogan's intense efforts, they did not lead to an end of the war. Moreover, the *balancer* act of Türkiye since the beginning of the war, need not be perceived as an unbiased one. As Russia's strength in Ukraine would decrease, Türkiye took on the advantage and replace it in terms of influence in the Southern Caucasus. In addition, it would be a good opportunity to replace Russia's influence in the Mediterranean and Syria, where the two – Türkiye and Russia, shared a strategic partnership for a while.

CONCLUSIONS

A first answer to the question posed in the introduction – *Is Türkiye an uncomfortable actor or a significant regional "balancer"?* inclines towards providing a confirmation of the second part of the question. The reason stands in the fact that, despite its uncomfortable regional and international manifestations, Türkiye managed, even in the form of small and short-lived victories, to maintain a form of regional balance. Its uncomfortable feature stems from a strong historical heritage and its imperial tradition, which for centuries dominated and thus changed the fate of the European continent. Even today, Türkiye is still in a position able to influence the evolution of the continent through the extent of its relationships with regional and international actors. A deeper answer would be that President Erdogan is perfectly aware of the role that Türkiye can play, at least on a regional level, and would not forfeit it.

While in domestic terms, 2023 was the year in which President Erdogan's etatism was defined, in foreign affairs terms, it was the year in which Türkiye advanced its efforts to lead to the end of the war in Ukraine. Despite the fact that some

of its actions did not bear fruit – see BSGI, and that it was accused of favouring Russia several times – due to their relationship in terms of energy and fuel, Türkiye was consistent in its support of Ukraine. As a result, one can claim Türkiye to be an uncomfortable, even difficult to deal with actor, due to its firm stand, but it is a *balancer* to the core, in the true sense of the word.

BIBLIOGRAPHY:

1. Aydogan, M. (2022). *Now it's time to focus on Ukraine cease-fire, says top Turkish diplomat,* AA.com: https://www.aa.com.tr/en/turkiye/now-its-time-to-focus-on-ukraine-cease-fire-says-top-turkish-diplomat/2647854, retrieved on 22 June 2024.
2. Christiansen, T.J., Snyder, J. (1990). *Chain Gangs and Passed Bucks: Predicting Alliance Patterns in Multipolarity*. International Organization, vol. 2, no. 44, pp. 137-168.
3. Coşkun, A., Ülgen, S. (2022). *Political Change and Turkey's Foreign Policy. Carnegie Endowment for International Peace,* https://carnegieendowment.org/files/Coskun_Ulgen_Turkey_final.pdf., retrieved on 22 July 2024.
4. Council of Europe (2017). *Turkey –Opinion on the amendments to the Constitution adopted by the Grand National Assembly on 21 January 2017 and to be submitted to a National Referendum on 16 April 2017.* Venice Commission: https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2017)005-e, retrieved on 23 June 2024.
5. Fella, S., Walker, N. (2023). *Turkey under Erdoğan: recent developments and the 2023 elections*, https://commonslibrary.parliament.uk/research-briefings/cbp-9806/., retrieved on 2 August 2024.
6. Focus Economics (2022). *Turkey Inflation*, https://www.focus-economics.com/country-indicator/turkey/inflation/, retrieved on 2 August 2024.
7. Gaber, Y. (2022). *How Turkey can play a more constructive role in Russia's war on Ukraine*. Atlantic Council, https://www.atlanticcouncil.org/blogs/turkeysource/how-turkey-can-play-a-more-constructive-role-in-russias-war-on-ukraine/, retrieved on 23 July 2024.
8. Gaber, Y. (2023). *One year into the war, it's time for Turkey to reconsider its Ukraine-Russia balancing act*. Atlantic Council, https://www.atlanticcouncil.org/blogs/turkeysource/one-year-into-the-war-its-time-for-turkey-to-reconsider-its-ukraine-russia-balancing-act/#:~:text=Since%20the%20start%20of%20Russia's,militarily%-20without%20alienating%20Russia%20economically, retrieved on 12 August 2024.
9. Haas, D. (2023). *Old enemies make new friends: Turkey in the Western Balkans*. Emerging Europe, https://emerging-europe.com/news/old-enemies-make-new-friends-turkey-in-the-western-balkans/, retrieved on 12 June 2024.
10. Human Rights Watch (2016). *A Blank Check. Turkey's Post-Coup Suspension of Safeguards Against Torture*, https://www.hrw.org/report/2016/10/26/blank-check/turkeys-post-coup-suspension-safeguards-against-torture, retrieved on 22 June 2024.
11. Khalifa, D., Waters, G. (2023). *Türkiye's Syria Policy after Erdoğan's Win*. International Crisis Group, https://www.crisisgroup.org/europe-central-asia/east-mediterranean/turkiye-syria/turkiyes-syria-policy-after-erdogans-win, retrieved on 2 August 2024.
12. Sanchez-Tapia, F. (2022). *The balancing act of Turkish foreign policy and the war in Ukraine – Analysis Paper*. Instituto Espanol de Estudios Estrategicos, nr=o.31:https://www.ieee.es/Galerias/fichero/docs_analisis/2022/DIEEEA31_2022_ENG.pdf., retrieved on 2 August 2024.
13. Sofuoglu, M. (2022). *Istanbul-based centre for Ukrainian grain exports a lifeline to humanity*. TRT World, https://www.trtworld.com/magazine/istanbul-based-centre-for-ukrainian-grain-exports-a-lifeline-to-humanity-59234, retrieved on 23 July 2024.
14. The Economist (2022). *Why Vladimir Putin and Recep Tayyip Erdogan need each other,* https://www.economist.com/europe/2022/10/12/why-vladimir-putin-and-recep-tayyip-erdogan-need-each-other, retrieved on 21 August 2024.
15. United Nations (2018). *Turkey: UN report details extensive human rights violations during protracted state of emergency*. United Nations, https://www.ohchr.org/en/press-releases/2018/03/turkey-un-report-details-extensive-human-rights-violations-during-protracted?LangID=E&NewsID=22853, retrieved on 17 July 2024.
16. Vasquez, J.A., Elman, C. (2012). *Realismul și balanța de putere*. Iași: Editura Polirom.
17. Waltz, K.N. (2006). *Teoria politicii internaționale*. Iași: Editura Polirom.

THE MIDDLE EAST IN THE FACE OF A PERFECT STORM – THE REGIONAL IMPACT OF ISRAEL-HEZBOLLAH CONFLICT –

Assistant Professor Adriana SAULIUC, PhD
"Titu Maiorescu" University, Bucharest;
Senior Researcher, Centre for Conflict Prevention & Early Warning, Bucharest
DOI: 10.55535/RMT.2024.4.32

The signing, in 2020, of the Abraham Accords and the events that followed fuelled the hope that developments in the Middle East could be marked by a cooperative relationship between the main regional rivals, but the fateful day of 7 October 2023 reshaped this space in a manner that inevitably led to a return to a state of confrontation. Thus, tensions in the region are raising fears that a major conflict, with international repercussions, is more a matter of "when" rather than "if" a major war will occur. This is due to the fact that, in the current tense regional context, the marking of about a year of the Hamas-Israel conflict largely coincides with the shift of the Israeli state's focus on the Hezbollah group, the low-intensity conflict between the two actors turning into one that has literally shaken not only Lebanon, but the entire region.

Keywords: conflict; Middle East; security; military/intelligence operations; MENA;

THE MIDDLE EAST – BETWEEN COOPERATION AND CONFRONTATION

More than a decade after the demonstrations and revolutions commonly known as the *"Arab Spring"* (Cordesman, 2020, p. 2), the Middle East is going through one of the most complicated stages (Simon, 2021), as a result of an interesting mix of elements influencing its evolution: alliances have been remodelled, the economic dimension is changing, while efforts aimed at resolving conflicts in the region seem far from achieving their goals. In other words, political, economic and social transformations, to which are added major challenges in the security field, make the region currently the hot spot on the world's political map. A powder keg close to the point of explosion, in the context in which the actions of regional actors further fuel tensions, tensions that in recent months have reached a dangerous point, generating fears that the region is on the edge of the abyss.

From the perspective of reshaping alliances, the most relevant developments are related to the Abraham Agreements, signed in 2020 (The Abraham Accords, 2020), which represented a historic moment in the relations of the Israeli state with the Arab countries with which it signed normalization agreements, meaning the United Arab Emirates, Bahrain, Morocco and Sudan. The importance of normalizing Israel's relations with the aforementioned states transcends the dimension of bilateral ties, being a moment with major implications for the entire Middle East and beyond.

A first aspect worth mentioning is the fact that the change in relations between Israel and the Arab states signatory to the Abraham Accords has modified the *"radiography"* of the MENA region, in the sense that it has put an end to the decades-long consensus among Arab states that any opening towards the Israeli state that implies a normalization of relations should come in the context of previously reaching a solution to the Palestinian-Israeli conflict.

Hence the interpretation of the signing of the Abraham Accords as a turning point in developments in the Middle East, being the first time that a number of Arab states prioritized their national interests, i.e. obtaining benefits in the economic and security fields, as a result of easing tensions at the regional level, to the detriment of fuelling them, and the implicit cancellation of any option that would support cooperation in the region.

But beyond the economic aspects, which aimed to open Israel up to the Arab countries that signed the normalization agreements, meaning the United Arab Emirates, Bahrain, Morocco and Sudan, and vice versa, their opening up to the Israeli state, which should have ensured economic benefits through joint infrastructure projects, cooperation in the field of renewable energy, tourism and cultural exchanges, the major interest of these countries was claimed by the security field (Even, Fadlon, Guzansky, 2020). In the sense that, beyond the non-military dimensions of the advantages that the normalization of Israel's relations with the aforementioned Arab states should have brought, the main concern of the signatory countries of the Abraham Accords is related to Iran, a state which, through *proxy* actors used at the regional level and Tehran's foreign policy directions, has generated fears regarding its ambitions in many countries from this complicated space. Among them are those signatories of the Abraham Accords, especially the Israeli state, countries concerned about Iran's nuclear ambitions, Tehran's options for action in the region and the fact that Iran, unstoppable in the earliest phase of its rise to regional power and possibly nuclear power, may become a much too inconvenient actor for the Sunni Muslim world and for Israel, in particular, so that in the more or less distant future, no conjunctural alliance or any other form of cooperation in the field of information exchange and in terms of military cooperation will be able to reduce the influence of the Iranian state in the region.

Thus, starting from fears regarding the growth of Iran's influence, the decision of the Arab states – the United Arab Emirates, Bahrain, Morocco and Sudan – to initialize the *"legitimization"* of Israel opened new horizons of cooperation in important areas, such as the economic and military, reducing the isolation in which the Israeli state has found itself at the regional level since its declaration of independence in 1948. Then, the fact that the Abraham Accords are considered a milestone in Middle East diplomacy is an indisputable matter (Ross, 2021), given that before the normalization of relations with the United Arab Emirates, Bahrain, Morocco and Sudan, Israel was a signatory to only two formal peace agreements – with Egypt, signed in 1979 (Treaty between Israel and Egypt, 1973) and with Jordan, signed in 1994 (Treaty of Peace between the Hashemite Kingdom of Jordan and the State of Israel, 1994).

Hence the interpretation that, after decades of deadlock in Israel's relations with Arab countries, its recognition by the signatory states of the Abraham Accords would commit the parties to a formula of cooperation never seen before, realigning the interests of state actors in the region, based on a pragmatic and strategic approach and less on one that was tributary to the *"traditional"* conflict in the region, which

maintained the enmity between Arab countries and the Israeli state at a level that affected stability and peace in the area.

Then, the Abraham Accords were followed by the *"grand reconciliation"* between Saudi Arabia and Iran brokered by China in March 2023 (Ottaway, 2023), when the regimes in Riyadh and Tehran decided to bury the hatchet of war and, implicitly, to put an end to a *"cold"* war-type confrontation that had been waged for decades, a war that kept the Middle East captive under the pressure of a regional competition modelled on the USA-USSR rivalry for global supremacy, which took place between 1946/1947 and 1991.

Subsequent discussions on the possibility of *"thawing"* Saudi Arabia-Israel relations, against the backdrop of common interests and regional geopolitical dynamics, gave the most optimists hope that the Middle East could take on a different face and that the state of tension and conflict in this space could be replaced by one of cooperation between the main regional international actors. The same ones which, until recent events involving the diplomacy, fuelled tensions in this area in a manner that has severely affected peace and stability in the region. Regarding the potential normalization of Saudi Arabia-Israel relations (Blanchard, 2024), two elements can be considered as reference points. First, the fact that both the Saudi monarchy and the Israeli state have common concerns regarding Iran's regional influence (exercised in particular through the actions of Tehran's *proxies*, the Hezbollah group and the Houthi rebels), as well as the Tehran regime's interest in nuclear weapons, despite the official Iranian position that supports a contrary situation.

But, unlike the signatory states of the Abraham Accords, Saudi Arabia, the pole of power of the Sunni Muslim world, conditioned the normalization of relations with the State of Israel on the resolution of the Palestinian issue, supporting the Saudi monarchy's commitment to *The Arab Peace Initiative of 2002* (Mekelberg, Shapland, 2018. pp. 7-8), initiative also known as the *"Abdullah plan"*, after the name of the crown prince at the time, Abdullah, who devised a series of steps aimed at solving the Palestinian problem. Specifically, under the auspices of this initiative, Saudi Arabia offered Israel the option of normalizing relations with the Arab world in exchange for a solution to the Palestinian problem that would involve the much-discussed and analysed two-state solution, with the Palestinians occupying the territory within the pre-1967 borders.

The Saudi position has changed over time, however, as a result of two events of utmost importance: first, the change of the Crown Prince of Saudi Arabia – in the person of Mohammed bin Salman starting with 2017, brought to the fore a (future)

pragmatic leader oriented towards the advantages of escaping from the pressure of extremely strict policies and decisions of the Saudi regime. Secondly, under the *de jure* leadership of King Salman and *de facto* of Crown Prince Mohammed bin Salman, Saudi Arabia has recently signalled that the Saudi kingdom would be willing to reconsider the aforementioned conditionality if negotiations with Israel had the potential to ensure the achievement of broader interests of the Saudi state (Al Jazeera, 2023).

Then, information appearing in the public space regarding the existence of non-public negotiations between the two states pushed the speculation even further and, despite the failure to reach an official agreement between Saudi Arabia and Israel, they indicated a possible evolution towards normalization of relations between the two countries. A situation that raised problems for the regime in Tehran, forced to (re)act in relation to a series of developments in strong contradiction with the Iranian strategic interests in the region, including the possible creation of a Saudi-Israeli *"common front"* against Iran's influence and ambitions, including nuclear ones. Not coincidentally, the next event with a major impact at the regional level is the fateful attack on 7 October 2023 of Hamas against the Israeli state, an attack inevitably followed by the outbreak of a conflict between the two international actors (Hamas and Israel) and which had as its first immediate consequence the blocking of any normalization initiatives at the regional level (Ulrichsen, 2023).

THE 7 OCTOBER 2023 TURNING POINT OPENS A BLOODY CHAPTER IN THE MIDDLE EAST

The surprise attack of the Hamas terrorist group against Israel (October 2023), with the unique feature that it took place within the borders of the Israeli state, has seriously damaged the sensitive regional balance resulting from the efforts made in recent years by the states in this area concerned with the stability and security of the region. Inevitably, following the Hamas attack, the results of these efforts collapsed like dominoes under the pressure of the consequences of the actions of the Palestinian terrorist group, at the same time triggering a *"witch hunt"* that Israel formally assumed, the goal being to eliminate the terrorist threat coming from Hamas (Eiran, 2023). At the same time, the involvement of Hezbollah, Iran's main *proxy* in the region, in the Palestinian terrorist group's fight against the Israeli state, starting on 8 October 2023, put the Israeli state in the position of expanding military missions beyond the Gaza Strip and combining, in a complex formula, military and intelligence-type actions, the result being the decimation and beheading of the Lebanese Shiite group Hezbollah.

Since, after the emergence of Hezbollah (1982), a group that assumed the fight against the Israeli state, military/intelligence actions against the Lebanese Shiite organization represented a major objective for Israel, the recent period has highlighted a certain preference of the Israeli state for the second dimension, without neglecting the military one (Elliott, 2024). In other words, pre-emptive strikes, which most often involved surgical airstrikes targeting Hezbollah military targets, meaning facilities, weapons depots, and arms supply convoys from Iran via Lebanon or Syria, have over time represented options that have brought Israel advantages in terms of material losses, and not only on the part of the Lebanese Shiite group.

Then, the war in Lebanon (12 July – 14 August 2006), represented a violent episode which was based on preventive actions initiated by the Israelis, while its conclusion left the issue between the two actors in an impasse that would not bode well for the more or less distant future (Byman, 2024). A fact validated by subsequent developments, which maintained the two regional international actors (Hezbollah and Israel) in a state of enmity, inevitably consumed in decades of armed confrontations of varying intensities and with varying frequencies.

Thus, the period that followed kept tensions on the border between Israel and Lebanon at a dangerous level, and after the conflict was triggered by Hamas, on 7 October 2023, Hezbollah decided to play a dangerous card, in the sense that it became involved, starting on 8 October 2023, in attacks on targets on the territory of the Israeli state, while trying to keep the level of actions against the State of Israel below a dangerous level, so as not to question the very existence of the Lebanese terrorist organization (Polak, 2024). But Hezbollah's calculations did not coincide with those of the Israeli military and intelligence structures, which recently launched an *"assault"* against the members and commanders of the Lebanese Shiite group, which has recently suffered major losses, including at the highest level of leadership.

ISRAEL VS. HEZBOLLAH - A DANGEROUS ZERO-SUM GAME

The positioning of the two actors on one side and the other of the barricade represents a reality that emerges from the very birth of the Lebanese Shiite group, which was formed in the 1980s with the aim of fighting against Israel. In such a context, Hezbollah's evolution was fuelled by hostility towards the Israeli state, hence the decades of tensions that in different guises and in different contexts reached dangerous levels that pushed the situation towards conflict, the case of the 2006 war, but also of the recent one, marked by an amplification of Israeli actions both in the intelligence and military fields.

Regarding the first dimension, the Israelis' preference for intelligence operations aimed at monitoring and infiltrating in order to counter Hezbollah activities is well known. The killing, on 30 July 2024, formally assumed by the State of Israel, of the so-called *"ghost of Hezbollah"* because of his extremely discreet activity, in the person of commander Fuad Shurk (Rasmussen, 2024), then the ingenious removal from the scene of a number of important Hezbollah operatives, by detonating their pagers (17 September 2024) and walkie-talkie communication stations (18 September 2024), actions that were attributed to Israel, which initially did not officially assume responsibility for them (Arab Center for Research and Policy Studies, 2024), the assumption coming not until 11 November 2024, reveals the Israelis' preference for actions that do not expose Israeli forces, which offers the important possibility of acting in secret and implicitly the option of assuming or not the responsibility for the respective actions by the leadership in Jerusalem.

Then, the military dimension represents a key element in Israel's fight against Hezbollah, and the elimination of the Secretary General of the Lebanese Shiite organization, Hassan Nasrallah, on 27 September 2024, following airstrikes that targeted the organization's headquarters located under residential buildings in the Dahieh suburb in the south of the Lebanese capital Beirut (Saab, 2024), while information appeared in the public space regarding the elimination of the one who was said to succeed Nasrallah, Hashem Safieddin (Christou, 2024), information unconfirmed by the group, indicates that, at least up to this point, the strategy used by Israel against Hezbollah, of the *"escalate de-escalate"* type, is showing its effectiveness.

Beyond the pragmatic aspects related to the concrete results of the actions taken by the Israelis in the intelligence and military fields, the recent developments involving the conflict between the two international actors – Israel and Hezbollah, reveal a return of the Israeli intelligence services to the leading position occupied prior to 7 October 2023, a date that marks a major failure recorded by Israeli intelligence as a result of the successful staging, by Hamas, of the most heinous attack on Israeli civilians on the territory of the State of Israel (Wyss, 2024).

Therefore, the resounding successes recorded by the Israelis in recent times against the enemies of the state, about which, despite the lack of clear information, there is certainty that they have more than prolific and ingenious intelligence work behind them, bring Israeli intelligence structures back into focus, but in a manner opposite to the perception created at the time of 7 October 2023, when the reputation of Israeli intelligence was strongly affected by the success and unpredictability of the Hamas attack. Now, in the context of Israel's recent actions, the undisputed aura of Israeli intelligence services before October 2023 has once

again become a reality that has brought back into focus the fearsome reputation they have for Israel's enemies, among which we can find, undoubtedly, Hezbollah.

Thus, in this life-and-death struggle, Israel positions itself pragmatically towards the Lebanese Shiite group, calibrating its actions and reaction to Hezbollah attacks according to the harsh rules of the zero-sum game, the same rules by which the Lebanese Shiite group establishes its position towards Israel. Inevitably, in such a context, the relationship between the two international actors can only remain stuck in the logic of confrontation, in which a military, strategic or political gain by one of the parties is perceived by the other as an unacceptable loss, hence the fuelling of a spiral of violence by the actions and countermeasures of both rival parties.

Then, the regional context does not currently offer other options for reducing tensions between Israel and Hezbollah, given that the Hamas attack in October 2023 has reshaped the Middle East in a way that a return to a *status quo ante* is impossible, the effects of the opening of the states in the area to cooperation and the level reached on this dimension in recent years being nullified by the return to a state of confrontation in the category of a zero-sum geopolitical game. Moreover, beyond the rhetoric of the Lebanese Shiite group that aims to hide the losses it has recorded, the reality is that Israel has achieved in few months a major advantage over Hezbollah that it has not been able to achieve in years, which makes it unlikely that the Israeli state will consider taking any step back and not make the most of the window of opportunity that has arisen in the fight against one of Israel's most prolific enemies.

THE ESCALATION TRAP

With a strategic stake that is far too high for the Israelis, while for Hezbollah it may also take on nuances related to the survival of the Lebanese Shiite group, the conflict between the two regional international actors remains caught in an *"escalation trap"*, given that its dynamics, marked by complexity and unpredictability as a result of the elements it involves, remains a destabilizing factor in the region, with the possible deterioration of the situation to an extremely dangerous point, which would also imply a rapid and uncontrolled intensification of the situation (Stroul, 2024). And the reasons why the conflict between Hezbollah and Israel can be explained in terms of an escalation trap are more than obvious:

the history of enmity, confrontations and tensions means that the two actors can only communicate through the language of violence. And it is particularly related to the fact that the emergence of Hezbollah, in the early 1980s, was based on the idea of resistance against the Israeli occupation of southern Lebanon, so that,

from the moment of the appearance of the Lebanese Shiite group until today, the history of relations between the two actors has been based on tensions and confrontation. Moreover, if in the case of Israel, which has regular Armed Forces, things are clear on the military dimension, in that of Hezbollah the particularity is that members of this group have accumulated relevant military experience in the conflicts in Syria, to which is added the support received from Iran, the result being the transformation of Hezbollah into the most relevant militant force in the region;

geographical proximity and strategic pressure – Hezbollah's positioning in southern Lebanon, which is in the area situated north of the Israeli-Lebanese border, as well as its operation in this area, reveals an extremely dangerous proximity between the two enemies, so that any action, incident or even miscalculation can be interpreted by both sides of the border in a bellicose approach, being perceived as a direct threat. Another aspect which complicates the security equation in this volatile space is the fact that Israel is extremely sensitive to any type of provocation from Hezbollah, as a result of the vulnerability it perceives in relation to the enemy due to the fact that the northern part of Israeli territory is inhabited by a civilian population, implicitly exposed to the threats generated by Hezbollah's actions;

Iran represents another destabilizing factor, as Hezbollah is known to be a *proxy* for Tehran, with the Iranian state formally assuming enmity towards Israel and its influence in the region. Hence Israel's strategy in the fight against Hezbollah, which is thought out in clear terms, in the sense that a weakening/annihilation of the Lebanese Shiite group is interpreted as being equivalent to weakening the Tehran regime's ability to act in the region and to act to the detriment of Israeli strategic interests;

the risk of miscalculation remains one of the concerns of regional international actors and the entire international community, given that Israel's military strategy reveals a preference for disproportionate military responses with the aim of deterring adversaries, hence the fear of a slide towards a major conflict in the region. On the other hand, Hezbollah has a reputation as a militant group built on resistance, which translates, in the simplest terms, into the fact that the Lebanese Shiite group will not give in to pressure from Israel, at least as long as it benefits from the support it receives from Tehran.

THE IMPACT OF DONALD TRUMP'S VICTORY IN THE US ELECTION ON THE CONFLICT BETWEEN HEZBOLLAH AND ISRAEL

The victory of the Republican candidate Donald Trump in the November 2024 presidential election in the United States of America will inevitably impact developments in the Middle East in a way that favours the Israeli state. Specifically, the deeply anti-Iranian approach during the first term in the White House is unlikely

to not put its mark on the US foreign policy during the second Trump Administration, which highlights a series of aspects that will have their effects on the Middle East in the years to come (Stack, 2024).

Thus, a first aspect is Washington's unconditional support for Israel, or more precisely the continuation of that shown during Trump's first term through decisions such as moving the United States Embassy to Jerusalem and recognizing Israeli sovereignty over the Golan Heights. A strong support on the political dimension will undoubtedly reverberate in the military field, its continuation representing an element that will contribute to raising the profile of the Israeli state in the region and implicitly the capacity to act against regional enemies, which translates into a possible increase in Israel's aggressiveness against Hezbollah and other Iranian proxies.

Inevitably, any pro-Israeli American support is interpreted in Tehran as additional pressure on Iran, especially since it is not excluded that the Iranian state will again come under a new set of sanctions that will further isolate this country on the international arena. The sanctions will economically cripple Iran, and their effects in the medium and long term bring into question the reduction of Tehran's ability to finance and arm Hezbollah and other militias, which inevitably provides an important strategic advantage to Israel.

Last but not least, it is possible that the United States' support for Israel will also involve regional actors, specifically Saudi Arabia and the Gulf countries, which future US President Donald Trump may consider from the perspective of creating a united anti-Iran and anti-Hezbollah approach, by resuming efforts to consolidate the Abraham Accords and by promoting a regional coalition to act against Iran's influence in the area through *proxy* actors and through Tehran's direct actions.

INSTEAD OF CONCLUSIONS

Taking into account all these aspects, meaning the realities in the region, the appetite of some international state and non-state actors in this space for the use of armed violence in order to solve the problems they face, as well as the change in the White House in January 2025, create the premises for developments that generate concern. It is due to elements that influence each other on the model of the butterfly effect found in chaos theory, from international to regional, but with the inevitable focus on the results of the elections in the United States of America, which is expected to translate into massive support for Israel and pressure on Iran starting in January 2025, which could evolve to a point where the conflict between the two international actors – Hezbollah and Israel – moves to a higher level of confrontation.

In another scenario, the desirable one, the future leader in the White House will avoid antagonizing the two aforementioned actors, emphasizing the non-military dimension of containing Iran, which would mean economic solutions and sanctions.

In either situation, Israel will try to achieve military victories against Hezbollah and Hamas, taking full advantage of the identified window of opportunity – a Biden Administration on the verge of departure and a Trump Administration preparing to take office, from which Israel has more expectations in terms of support for sensitive regional files.

BIBLIOGRAPHY:

1. Al Jazeera (2023). *Saudi Crown Prince MBS says Israel normalisation getting 'closer'*, https://www.aljazeera.com/news/2023/9/20/saudi-crown-prince-mbs-says-israel-normalisation-getting-closer, retrieved on 24 September 2024.
2. Arab Center for Research and Policy Studies (2024). *Israel Signals Escalation with Attacks on Hezbollah Communications Devices,* https://www.dohainstitute.org/en/Lists/ACRPS-PDFDocumentLibrary/pager-massacre-implications-for-lebanon.pdf., retrieved on 29 September 2024.
3. Blanchard, C.M. (2024). *Possible U.S.-Saudi Agreements and Normalization with Israel: Considerations for Congress.* Congressional Research Service, https://crsreports.congress.gov/product/pdf/R/R48162., retrieved on 20 September 2024.
4. Byman, D. (2024). *Lessons from Israel's Last War in Lebanon.* Center for Strategic and International Studies, https://www.csis.org/analysis/lessons-israels-last-war-lebanon, retrieved on 27 September 2024.
5. Christou, W. (2024). *Israel confirms killing of Hashem Safieddine, presumed next leader of Hezbollah*. In *The Guardian*, https://www.theguardian.com/world/2024/oct/22/israel-confirms-killing-of-presumed-next-leader-of-hezbollah, retrieved on 29 September 2024.
6. Cordesman, A.H. (2020). *The Greater Middle East: From the "Arab Spring" to the "Axis of Failed States"*. Center for Strategic and International Studies, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200824_MENA_Axis_Failed_States.pdf., retrieved on 12 September 2024.
7. Eiran, E. (2023). *Israel's failures and response to the Hamas attack: A preliminary assessment*. Middle East Institute, https://www.mei.edu/publications/israels-failures-and-response-hamas-attack-preliminary-assessment, retrieved on 27 September 2024.
8. Elliott, M. (2024). *Israel is Trying to Move Beyond Deterrence with Hezbollah*. Stimson, https://www.stimson.org/2024/israel-is-trying-to-move-beyond-deterrence-with-hezbollah/, retrieved on 27 September 2024.
9. Even, S., Fadlon, T., Guzansky, Y. (2020). *The Economic-Strategic Dimension of the Abraham Accords.* The Institute for National Security Studies, https://www.inss.org.il/publication/abraham-accords-economic-dimension/, retrieved on 15 September 2024.
10. Mekelberg, Y., Shapland. G. (2018). *Israeli-Palestinian Peacemaking What Can We Learn From Previous Efforts?.* Middle East and North Africa Programme. Chatham House, https://www.chathamhouse.org/sites/default/files/publications/research/2018-07-24-israeli-palestinian-peacemaking-mekelberg-shapland.pdf., retrieved on 24 September 2024.
11. Ottaway, D. (2024). *Saudi-Iranian Relations Restored but Remain Tense.* Wilson Center, https://www.wilsoncenter.org/article/saudi-iranian-relations-restored-remain-tense., retrieved on 20 September 2024.
12. Polak, D. (2024). *Analysis of The Intensity and Range of Hezbollah Attacks on Israel (October 8, 2023 – October 1, 2024)*. Alma Research and Education Center, https://israel-alma.org/2024/10/10/analysis-of-the-intensity-and-range-of-hezbollah-attacks-on-israel-october-8-2023-october-1-2024/, retrieved on 27 September 2024.
13. Rasmussen, S.E. (2024). *How Israel Killed a Ghost.* In The Wall Street Journal, https://www.wsj.com/world/middle-east/how-israel-killed-a-ghost-73e6db68, retrieved on 29 September 2024.
14. Ross, D. (2021). *The Abraham Accords and the Changing Shape of the Middle East.* The Washington Institute for Near East Policy, https://www.washingtoninstitute.org/policy-analysis/abraham-accords-and-changing-shape-middle-east, retrieved on 20 September 2024.
15. Saab, B.Y. (2024). *Hezbollah faces an uncertain future after the assassination of Hassan Nasrallah*. Chatham House, https://www.chathamhouse.org/2024/10/hezbollah-faces-uncertain-future-after-assassination-hassan-nasrallah, retrieved on 29 September 2024.
16. Simon, C. (2021). *10 years later: Was the Arab Spring a failure?.* In *The Harvard Gazette*, https://news.harvard.edu/gazette/story/2021/02/ten-years-later-was-the-arab-spring-a-failure/, retrieved on 12 September 2024.
17. Stack, L. (2024). *Trump Has History of Strong Support for Israel*. In *The New York Times,* https://www.nytimes.com/2024/11/06/world/middleeast/trump-israel-support.html, retrieved on 29 September 2024.
18. Stroul, D. (2024). *Israel and Hezbollah Are Escalating Toward Catastrophe*. The Washington Institute for Near East Policy, https://www.washingtoninstitute.org/policy-analysis/israel-and-hezbollah-are-escalating-toward-catastrophe, retrieved on 29 September 2024.
19. The Abraham Accords (2020). U.S. Department of State, https://www.state.gov/the-abraham-accords/, retrieved on 15 September 2024.
20. *Treaty between Israel and Egypt* (1973). Yale Law School, Lillian Goldman Law Library, https://avalon.law.yale.edu/21st_century/isregypt.asp., retrieved on 20 September 2024.
21. *Treaty of Peace between the Hashemite Kingdom of Jordan and the State of Israel* (1994). The Library, http://www.kinghussein.gov.jo/peacetreaty.html, retrieved on 20 September 2024.
22. Ulrichsen, K.C. (2023). *Saudi-Israeli Normalization and the Hamas Attack.* Arab Center Washington D.C., https://arabcenterdc.org/resource/saudi-israeli-normalization-and-the-hamas-attack/., retrieved on 26 September 2024.
23. Wyss, M. (2024). *The October 7 Attack: An Assessment of the Intelligence Failings.* The Combating Terrorism Center at West Point, https://ctc.westpoint.edu/the-october-7-attack-an-assessment-of-the-intelligence-failings/, retrieved on 29 September 2024.

RUSSIA-UKRAINE WAR OF DRONES – STRATEGIC IMPACT, TACTICS, AND IMPLICATIONS. THE DRONES DROPPED IN ROMANIA DURING THE RUSSIA-UKRAINE WAR –

Navy Captain (ret.) Associate Professor Romeo BOȘNEAGU
"Mircea cel Bătrân" Naval Academy, Constanţa
DOI: 10.55535/RMT.2024.4.33

The Russia-Ukraine war has demonstrated the increasing importance of unmanned aerial vehicles (UAVs), commonly known as drones, in modern warfare. Drones have been pivotal in reconnaissance, surveillance, targeting, and direct strikes, altering the tactical and strategic landscape of the conflict. This paper examines the types of drones used by both Russia and Ukraine, their operational roles, technological advancements, and the implications for future warfare. The use of drones in the war illustrates both their capabilities and vulnerabilities, providing lessons for military strategists and policymakers worldwide. The incidents of drones dropping in Romanian territory during the Russia-Ukraine war highlight the complex and often unpredictable nature of modern warfare, where technology, geography and geopolitics intersect in challenging ways. These incidents underscore the risks of escalation and miscalculation in a conflict that already threatens regional and global security.

Keywords: unmanned aerial vehicles/UAVs; Ukraine; war; technology; impact;

INTRODUCTION

Since the Russian invasion of Ukraine in February 2022, the conflict has involved various military tactics and technologies, including the extensive use of drones for surveillance, reconnaissance, and attack. Both Russia and Ukraine have deployed a wide range of unmanned aerial vehicles (UAVs) to achieve tactical and strategic objectives, such as gathering intelligence, targeting enemy positions, and delivering payloads. The use of drones has become a crucial element of modern warfare due to their cost-effectiveness, versatility, and ability to operate in contested airspace without risking human life.

Drones have emerged as crucial tools in contemporary warfare, offering unique advantages in terms of surveillance, reconnaissance, and targeted attacks. The ongoing conflict between Russia and Ukraine has underscored the growing significance of drones in both offensive and defensive operations. Since the beginning of the conflict in 2014, drones have played an increasingly prominent role, with both sides deploying a variety of UAVs for different tactical purposes. This paper explores the use of drones in the Russia-Ukraine war, highlighting their strategic impact, operational roles, and the broader implications for military operations *(figure 1)*.

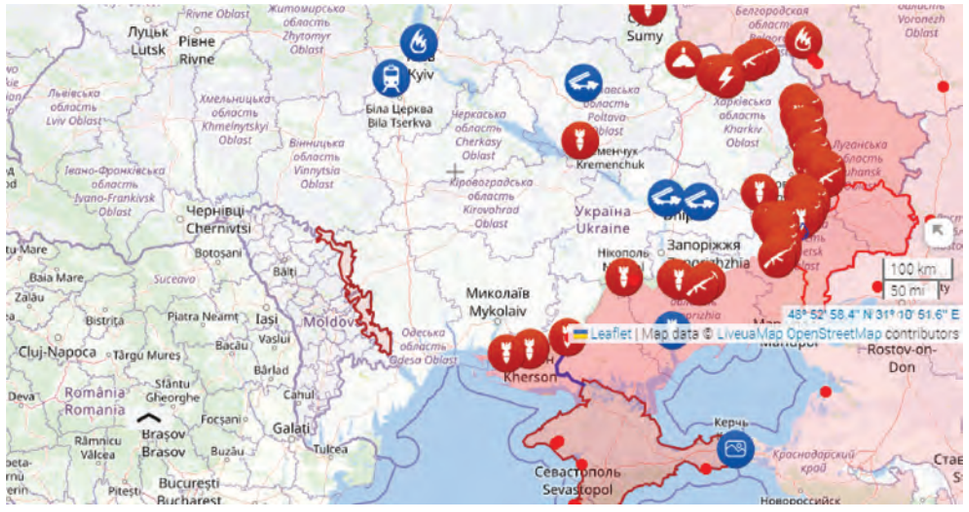


Figure 1: Map of Ukraine indicating areas of drone operations and major battles, 9 September 2024 (https://liveuamap.com)

TYPES OF DRONES USED BY RUSSIA AND UKRAINE

Ukrainian Drones

Ukraine has utilized a range of drones for surveillance, reconnaissance, and strike missions, mentioned in *table 1*.

Table 1: Drones used by Ukraine (Sotoudehfar, Sarkin, 2024)

Drone	Made in	Type Function
Bayraktar (TB2)	Türkiye	Military ISR, Targeting, Strike missions
Phoenix Ghost	USA	Military Loitering munitions, Surveillance
WB Group Warmate	Poland	Military ISR, Loitering
RAM II	Ukraine	Military Loitering
Spectator-M1	Ukraine	Military Reconnaissance, Search, Rescue
UJ-22 Airborne	Ukraine	Military Intelligence, Search, Rescue
Punisher	Ukraine	Military Strike military targets
Leleka-100 (stork)	Ukraine	Military & Commercial Reconnaissance, Surveillance, Target acquisition
Athlon Avia A1-CM Furia	Ukraine	Military Reconnaissance, Surveillance
R18	Ukraine	Military Surveillance, Search, Delivery of cargo, Inflicting damage
Autel Evo II	China	Commercial Photography, Videography, Inspection, Mapping
DJI Mavic Series	China	Commercial Photography, Videography, Search, Rescue
Golden Eagle	USA	Commercial Surveillance
Skydio X2	USA	Commercial Search, Inspection, Rescue Mapping
PD-1 (People's Drone)	Ukraine	Military Reconnaissance, Monitoring, Anti-jamming
WB FlyEye	Poland	Military Unknown
Quantum System Vector	Germany	Commercial ISR
RQ-20 Puma	USA	Military ISR
Tupolev Tu-143 Reis	Former Soviet Union	Military Reconnaissance, Surveillance AeroVironment Quantix Inspection

Drone	Made in	Type Function
Mini-Bayraktar	Türkiye	Military Reconnaissance, Surveillance
Switchblade 300	USA	Military Reconnaissance, surveillance, Target acquisition, Loitering
Switchblade 600	USA	Military Loitering munition

Notable among them is the Turkish-made *Bayraktar TB2*, a medium-altitude, long-endurance (MALE) drone capable of both surveillance and precision strikes. The Bayraktar TB2 *(table 2 and figure 2)* has been highly effective in targeting Russian armoured vehicles, artillery, and supply lines, earning it a reputation as a *"game-changer"* in the conflict (Kamp, 2022).

Table 2: Bayraktar Technical Specifications (https://baykartech.com/en/uav/bayraktar-tb2/)

Fully Automatic Navigation and Route Tracking Feature	Operational - Maximum Altitude	16.000 -22.000 feet	Payload - Munitions	4 Laser Guided Smart Ammunition
Precise Auto Take-off and Landing with Built-in Sensor Fusion	Payload Capacity	145 kg	Engine	100 hp (Gasoline)
Fully Automatic Taxi and Parking Feature	Travel - Maximum Speed	70 knot - 120 KTAS	Endurance	20+ hours
Semi-Autonomous Flight Modes Support	Take Off/ Landing/Cruise/ Taxi	Autonomous	Length	6.5 m
Fault Tolerant and 3 Redundant Sensor Fusion Application	MTOW	700 kg	Payload - ISR	Switchable EO/IR/LD or Multi-Purpose AESA Radar
Cross Redundant YKI System	Height	2.2 m		
Unique Redundant Servo Actuator Units	Wingspan	12 m		
Unique Redundant Lithium-Based Battery Units	Communication Range	LOS & BLOS		



Figure 2: Bayraktar TB2 Drone
(https://baykartech.com/en/uav/bayraktar-tb2/)

Ukraine has also developed its indigenous UAV capabilities. The PD-1 and PD-2 drones, produced by the Ukrainian company *Ukrspecsystems*, have been used for both surveillance and artillery spotting missions. These drones are relatively small, making them harder to detect and intercept by enemy air defences.

Russian Drones

Russia has deployed a diverse array of UAVs in its military operations against Ukraine as it can be seen in *table 3*.

Table 3: Drones used by Russia (Sotoudehfar, Sarkin, ib.)

Drone	Made in	Type Function
Zala	Russia	Military ISR, Kamikaze
Shahed136 (Geran-2)	Iran	Military Kamikaze
Mohajer 6	Iran	Military ISR, Air to ground strike
Orlan-10	Russia	Military ISR, Jamming
Orion	Russia	Military ISR, TA, Battle damage assessment
KBLA-IVT	Russia	Military Aerial target, Reconnaissance
Forpost	Russia	Military ISR
Zala	Russia	Military ISR
Granat-4	Russia	Russia Military ISR
Orlan-30	Russia	Military Reconnaissance, Surveillance
E95 (E95M)	Russia	Military Aerial target, Reconnaissance
Zastava	Russia & Israel	Military Reconnaissance
Tachyon	Russia	Military Reconnaissance
Eleron-3	Russia	Commercial Reconnaissance

They include the *Orlan-10*, a versatile reconnaissance drone, and the *ZALA Aero*, designed for electronic warfare and intelligence gathering. The Orlan-10, in particular, has been widely used for directing artillery fire and gathering intelligence on Ukrainian positions (Komarov, 2023).

The *Orlan-10* complex consists of unmanned aerial vehicles, launch and recovery systems, ground control segment, and swappable payloads. The UAV features modular design with high-wing configuration, while its tail section comprises a tailplane and a vertical stabiliser. It has a wingspan of 3.1 m and its aerodynamic fuselage is 2-m long. The empty weight and maximum take-off weights of the UAV are 12.5 kg and 16.5 kg respectively *(figure 3)*. The drone is launched using a collapsible catapult and recovered using a parachute landing system. The UAV's modular design is provided with several interchangeable payloads allowing for increased mission flexibility. It carries a day-light camera, a thermal imaging camera, a video camera and a radio transmitter in a gyro-stabilised camera pod that is fitted under the fuselage. The cameras provide real-time intelligence, 3D maps, surveillance, and aerial reconnaissance of ground-based targets. The imagery, video and other sensor data collected by the payloads are transmitted to the ground control station in real-time, through a data link using 3G/4G cellular networks. The *Orlan-10* is fitted with electronic warfare capability and can differentiate between friendly and enemy means of transmitting information. It can mount interference transmitters and set up zones for cellular jamming. Russia's drone arsenal also includes the *Forpost*, a license-produced version of the Israeli *Searcher II*, which has been used for long-range reconnaissance missions. Moreover, Russia has integrated the use of loitering munitions, such as the Lancet and KUB-BLA, to conduct precision strikes against Ukrainian targets (TASS, 2023).



Figure 3: Orlan 10 Drone
(https://www.airforce-technology.com/projects/orlan-10-unmanned-aerial-vehicle-uav/?cf-view)

Russian forces have deployed various types of drones (unmanned aerial vehicles or UAVs) in their military operations in Ukraine. These drones serve multiple purposes, including surveillance, reconnaissance, electronic warfare, and direct attacks. The most commonly used Russian drones in the conflict include:

- Orlan-10: A versatile, medium-range drone primarily used for reconnaissance, surveillance, and electronic warfare. The Orlan-10 can fly at altitudes of up to 5,000 meters and has an operational range of about 120 kilometres. It is equipped with cameras, infrared sensors, and communication jammers, making it valuable for gathering intelligence and disrupting enemy communications.
- Shahed-136 (Geran-2): While of Iranian origin, the Shahed-136 has been heavily used by Russian forces under the local designation Geran-2. This loitering munition, or *"kamikaze"* drone, is designed to dive into its target with a payload of explosives, making it a potent tool for attacking fixed positions, infrastructure, and enemy concentrations.
- Forpost: A medium-altitude, long-endurance UAV, based on the Israeli IAI Searcher II, the Forpost is employed for both surveillance and combat missions and can carry various payloads, including cameras and electronic warfare equipment. It is capable of flying for up to 17 hours, providing extended operational capacity for Russian forces.
- Eleron-3: A lightweight, short-range drone used for tactical reconnaissance. The Eleron-3 is launched by hand or from a catapult and is used for close-range missions to provide real-time intelligence to ground units.
- ZALA Lancet: Another loitering munition, the ZALA Lancet, is a small, fast, and relatively inexpensive drone capable of hitting both stationary and moving targets. It has been used for precision strikes against specific targets, such as vehicles and artillery positions.

These drones have been deployed in various capacities throughout the conflict, contributing significantly to Russian operations along Ukraine's southern and eastern fronts, including areas near the Romanian border.

OPERATIONAL ROLES OF DRONES IN THE CONFLICT

Surveillance and Reconnaissance

Drones have been extensively used for surveillance and reconnaissance by both sides. The ability to gather real-time intelligence and monitor enemy movements has been crucial in a conflict characterized by rapid changes on the ground. Ukrainian forces have used drones to identify and locate Russian troops and artillery positions, enabling more accurate targeting by artillery and ground forces (Bender, 2022).

Similarly, Russian drones have played a vital role in gathering intelligence on Ukrainian defences, spotting for artillery, and assessing the impact of strikes. The use of drones for continuous surveillance has allowed both sides to maintain a persistent *"eye in the sky"*, enhancing situational awareness and battlefield transparency (Carroll, 2022).

Targeting and Precision Strikes

Drones have also been employed for direct strikes, especially by Ukrainian forces using *Bayraktar TB2s* to target Russian tanks, artillery, and logistics. Videos released by the Ukrainian Ministry of Defence have shown numerous successful strikes against Russian convoys and positions, demonstrating the effectiveness of drones in degrading the enemy's combat capabilities (Kyiv Independent, 2023) *(Figure 4)*.



Figure 4: A drone equipped with an incendiary mixture captured the edge of the woods and began burning it meter by meter (Schcherbak, 2024)

On the Russian side, loitering munitions, such as the Lancet, have been used to target Ukrainian artillery and air defence systems. These drones, also known as *"kamikaze drones"*, can loiter over a target area and strike when an opportunity presents itself, adding a new dimension to precision warfare (Defense Express, 2023).

FACTORS INFLUENCING DRONE EFFECTIVENESS IN THE WAR

Technological Advancements

Technological advancements have greatly enhanced the capabilities of drones used in the conflict. Drones such as the *Bayraktar TB2* are equipped with advanced sensors, cameras, and precision-guided munitions, allowing them to strike targets with high accuracy. Electronic warfare capabilities, such as jamming and spoofing, have also been used to protect drones from enemy air defences (Grossman, 2022).

Countermeasures and Vulnerabilities

Despite their effectiveness, drones are not invulnerable. Both sides have deployed various countermeasures, including electronic warfare systems, anti-aircraft guns, and surface-to-air missiles, to neutralize enemy drones. In several instances, Ukrainian and Russian drones have been shot down or jammed, highlighting the challenges and vulnerabilities associated with drone warfare (Roblin, 2022).

Tactical and Strategic Impact

The tactical and strategic impact of drones in the Russia-Ukraine war has been significant. Drones have provided both sides with real-time intelligence, improved targeting accuracy, and the ability to conduct precision strikes with minimal risk to personnel. The psychological impact of drone strikes on both military personnel and civilian populations cannot be underestimated, as drones have become symbols of persistent surveillance and sudden, unpredictable attacks (Bachmann, 2022).

In the context of International Humanitarian Law (IHL), it is not solely the drones' technology itself, but rather the combination of unmanned systems and their advanced capabilities that make them a critical issue for IHL. The autonomy and precision of drones, along with their ability to conduct surveillance and strike with reduced or no human intervention, introduce unique challenges for international law. Drones possess a level of autonomy that differentiates them from traditional weaponry.

REGIONS IN UKRAINE NEAR ROMANIA ATTACKED BY RUSSIAN FORCES

Several Ukrainian regions near the Romanian border have been subjected to Russian drone and missile attacks since the beginning of the war. The following regions are particularly relevant due to their proximity to Romania:

- a. Odesa Oblast: Located along the Black Sea coast, Odesa is a crucial port region for Ukraine. Russian forces have frequently targeted Odesa

with missile strikes, drone attacks, and bombardments, aiming to disrupt Ukrainian logistics and supply lines and damage critical infrastructure, including grain storage facilities and ports.

- b. Vinnytsia Oblast: This region, while not directly on the Romanian border, is relatively close and has seen sporadic Russian missile and drone strikes. The strikes have targeted military facilities, transportation infrastructure, and civilian areas, leading to significant damage and casualties.
- c. Chernivtsi Oblast: While Chernivtsi is not a primary target of the war, its proximity to Romania makes it a potential area of concern. As of now, it has not experienced direct attacks, but the presence of military activity nearby has heightened the region's alert status.
- d. Zakarpattia Oblast: Like Chernivtsi, Zakarpattia has remained relatively unscathed by direct attacks. However, its strategic location along the Ukrainian border with Romania and other NATO members means any spillover of conflict could have significant implications.

Specific Incidents of Drone Parts Dropping in Romania

The ongoing conflict between Russia and Ukraine has not only profoundly affected the countries directly involved but has also sent shockwaves across the region, particularly in Eastern Europe. A recent and concerning development in this conflict has been the unintentional dropping of drones in Romanian territory. As a member of the North Atlantic Treaty Organization (NATO) and the European Union, Romania's involvement adds a complex layer to the already tense geopolitical situation. This paper examines the circumstances surrounding the drones that have been dropping in Romania, the potential causes and motivations behind these incidents, the broader geopolitical implications, and the challenges they present to regional security and international relations.

There have been several reported incidents where parts of Russian drones have dropped or been discovered in Romanian territory, raising concerns about potential escalation:

- First Incident: September 2023: The first significant incident occurred in early September 2023, when Romanian authorities discovered debris from a drone near the village of Plauru, close to the Danube River. The drone was identified as a part of a Russian Shahed-136 (Geran-2) loitering munition. This incident coincided with intensified Russian attacks on Ukrainian ports along the Danube, particularly near Izmail and Reni, which are very close to the Romanian border.

- Second Incident: Mid-September 2023: Another incident occurred in mid-September when additional drone debris was found near the village of Ceatalchioi, in the Tulcea region of Romania. The debris was linked to a Russian drone attack on Ukrainian infrastructure along the Danube River. Romanian officials expressed serious concern over these findings, as they represented a potential threat to Romanian territorial integrity and NATO's security.
- Subsequent Incidents: October and November 2023: Further incidents were reported in October and November 2023, where Romanian authorities discovered additional parts of Russian drones in areas near the Ukrainian border. The Romanian government, in collaboration with NATO, initiated investigations to determine the cause and intent of these incidents, but the findings remained inconclusive as to whether they were accidental or deliberate provocations.

Russian Attacks Near the Romanian Border: Frequency and Impact

Russian forces have launched numerous drone and missile attacks on Ukrainian targets near the Romanian border. The most significant attacks occurred during the following periods, reported by the international media:

- August 2023: Russian forces began increasing drone and missile attacks on Ukrainian ports along the Danube River, particularly targeting the ports of Izmail and Reni. These attacks aimed to disrupt Ukraine's grain exports following the collapse of the Black Sea Grain Initiative, which had allowed Ukrainian grain to reach international markets.
- September 2023: Attacks continued throughout September, with multiple strikes reported near the Danube ports. During that period, parts of drones used in these attacks were discovered on Romanian soil, suggesting that some drones may have overshot their targets or been downed by Ukrainian air defences, drifting into Romanian territory.
- October-November 2023: The frequency of attacks remained high, with ongoing strikes against Ukrainian infrastructure along the Danube. The attacks caused significant damage to port facilities, grain silos, and energy infrastructure, prompting continued concerns about the security of Romanian airspace and the potential for further spillover incidents.

The Romanian media has reported the following incidents related to the consequences of Russian drone attacks on Ukrainian regions near the Romanian border:

- 9 September 2023 – the President of Romania announces, *"Today's identification by the Romanian authorities on Romanian territory, near the border with Ukraine, of new drone fragments, similar to those used by the Russian military, indicates that an absolutely unacceptable violation of the sovereign airspace of Romania, a NATO ally state, has taken place, with real risks to the security of Romanian citizens in the area"*.
- 11 October 2023 – a new Russian kamikaze drone is discovered in Romania, after a new Russian bombing of Ukrainian ports on the Danube in the Odessa region;
- 14 December 2023 – a new drone crashes in Romania, in an uninhabited perimeter about 4 km upstream from the village of Grindu in the border area with Ukraine, the Ministry of National Defence announces.
- 9 to 10 February 2024 – Authorities in Tulcea and Galați Counties issue three Ro -Alert messages and F-16 fighter jets are deployed to monitor the situation after Russian forces execute drone strikes on Ukrainian port infrastructure at Izmail and Reni, near the Ukrainian-Romanian border.
- 25 July 2024 – The Ministry of Defence announces that it has found debris from a Russian-origin Geran1/2 drone near Plauru, Tulcea County.
- 20 August 2024. Specialists of the Romanian Ministry of National Defence have picked up fragments of a drone crashed at the end of July on the Romanian Danube bank after Russian attacks on port infrastructure in Ukraine.

Damages and Casualties from Russian Drone Attacks Near Romania

The Russian drone and missile attacks on Ukrainian targets near the Romanian border have caused considerable damage and casualties:

- Damage to Infrastructure: The attacks have primarily targeted critical infrastructure, including port facilities, grain storage silos, fuel depots, and energy installations. Ukrainian authorities reported significant damage to the port facilities in Izmail and Reni, which are vital for Ukraine's grain export routes. These attacks have disrupted shipping operations and inflicted substantial economic losses on Ukraine, affecting global grain markets.

- Casualties: Ukrainian officials reported several civilian casualties, including deaths and injuries, resulting from the drone and missile attacks near the Danube ports. In August and September 2023, at least 10 people were reported killed, and dozens were injured in strikes on Izmail and Reni. The continued assaults have strained local emergency services and prompted evacuations in some areas.
- Spillover Effects on Romania: Although there have been no direct casualties or damage reported in Romania from the drones that dropped on its territory, the incidents have increased security concerns. The Romanian government has taken steps to bolster its air defences along the border, and NATO has expressed its commitment to defending Romanian sovereignty and airspace, highlighting the risks of potential escalation.

Possible Causes and Motivations

The dropping of drones in Romanian territory could result from several factors, including misfires, technical malfunctions, or deliberate actions. Below are some potential causes and motivations behind these incidents:

- Accidental Intrusion Due to Malfunction: One plausible explanation is that these drones inadvertently strayed into Romanian airspace due to technical malfunctions or loss of control. The proximity of Romanian territory to active combat zones in Ukraine, particularly near the Danube River, means that drones operating in this area might unintentionally cross borders.
- Targeting Errors During Operations: The complexity of drone warfare and the dynamic nature of aerial engagements could result in targeting errors. Drones engaged in reconnaissance or attack missions over Ukrainian territory might, due to navigation errors or disrupted control signals, end up in Romanian airspace.
- Deliberate Provocation or Testing NATO's Response: Another possibility is that the drones entering Romanian airspace could be a deliberate attempt by Russia to test NATO's response. Given Romania's status as a NATO member, such incidents could be intended to gauge the alliance's readiness and resolve or to create uncertainty and tension within NATO ranks.
- Use of Romania as a Safe Haven: There is also speculation that some of these drones could be attempts by Ukrainian forces to escape Russian detection or interception by briefly entering Romanian airspace, thus leveraging NATO

territory as a *de facto* safe zone. However, this remains purely hypothetical and has not been substantiated by concrete evidence.

Geopolitical and Security Implications

The repeated dropping of drones in Romania has significant implications for regional security and international relations, particularly concerning NATO's role in the conflict and its commitment to collective defence under Article 5 of the NATO Treaty:

- Threat to NATO's Collective Defence Principle: The presence of drones in Romanian territory raises concerns about the potential escalation of conflict. If an incident were to be interpreted as an attack or deliberate provocation against a NATO member, it could trigger the alliance's collective defence mechanism, which could lead to a broader confrontation with Russia.
- Impact on Regional Security Dynamics: Romania is geographically positioned at a critical juncture in Eastern Europe. Incidents involving drones could destabilize the region, increase tensions between NATO and Russia, and prompt neighbouring countries, such as Bulgaria, Hungary, and Republic of Moldova, to reassess their security postures.
- Implications for NATO's Strategic Posture: The incidents challenge NATO's strategic calculations. On the one hand, NATO must demonstrate a commitment to defending its members' airspace and territorial integrity. On the other hand, it must avoid direct engagement with Russia that could escalate into a broader conflict. This delicate balance complicates NATO's military and diplomatic responses.
- Heightened Risk of Miscalculation: The unintentional or accidental dropping of drones on Romanian soil raises the risk of miscalculation or unintended escalation. Such incidents can be misconstrued, especially in a high-stress environment, leading to actions that might inadvertently widen the conflict. The uncertainty surrounding these incidents makes it difficult for policymakers to craft clear and decisive responses.

Romania's Response and NATO's Actions

In response to these drone incidents, Romania has taken several precautionary measures to safeguard its airspace and territory:

- Increased Surveillance and Monitoring: Romanian authorities, in cooperation with NATO, have heightened surveillance and monitoring of their airspace,

especially along the border with Ukraine. It includes deploying additional radar systems, aerial patrols, and advanced detection technologies.

- Diplomatic Measures: Romania has lodged formal protests with Russia over the incidents and has called for investigations to determine the precise origins and intentions behind the drones. The Romanian government has also engaged with NATO and EU partners to coordinate responses and seek assurances of collective security.
- Military Preparedness: Romania has increased its military readiness, conducting air defence drills and coordinating with NATO forces deployed in the region. Romanian air defence units have been placed on heightened alert to respond swiftly to any potential threats.
- Coordination with Allies: NATO has expressed solidarity with Romania and affirmed its commitment to protecting its members' sovereignty and territorial integrity. The alliance has conducted joint exercises in the Black Sea region, demonstrating its readiness to counter any threats.

Challenges in Addressing Drone Incidents

The incidents involving drones in Romania present several challenges for both Romanian authorities and NATO:

- Attribution Difficulties: Determining the origin and intent of the drones is complicated, especially in a contested airspace where multiple actors operate similar UAV technologies. The lack of definitive proof makes it challenging to assign blame or take decisive action.
- Legal and Diplomatic Complexities: Engaging in a military response against perceived provocations carries significant legal and diplomatic risks, particularly when operating under international law and NATO rules of engagement. Romania must balance the need to protect its airspace with the imperative to avoid escalation.
- Technological Limitations: Detecting and neutralizing drones, especially those designed with low radar cross-sections or advanced evasion capabilities, require sophisticated technology and infrastructure. Ensuring adequate coverage and response capability across the vast border region is a daunting task.

CONCLUSIONS

The use of drones in the Russia-Ukraine war has revolutionized modern warfare, providing strategic advantages in surveillance, targeting, and precision strikes. Both sides have effectively leveraged drones to enhance their operational capabilities, although they remain vulnerable to countermeasures. The conflict has demonstrated the transformative potential of drone technology and its implications for future military operations. As the war continues, the development and deployment of drones will likely shape the future of warfare in unprecedented ways.

The incidents of drones dropping in Romania during the Russia-Ukraine war underscore the complex and volatile nature of modern warfare, where the use of advanced technology like UAVs can have unintended consequences beyond the immediate battlefield. The presence of Russian drone debris in Romanian territory raises serious concerns about regional security, the potential for accidental or deliberate escalation, and the challenges of maintaining NATO's collective defence posture in an unpredictable conflict environment.

As Russian attacks on Ukrainian targets near the Romanian border continue, the international community, especially NATO, faces the delicate task of balancing support for Ukraine with the need to prevent further spillover of the conflict into member states' territories. Continued vigilance, diplomacy, and strategic planning will be essential to managing these risks and avoiding an escalation that could draw more countries into the conflict.

For Romania and its NATO allies, these events necessitate careful deliberation, robust diplomatic engagement, and increased vigilance to protect territorial sovereignty while avoiding unnecessary escalation. As the war in Ukraine continues, the potential for further incidents remains high, making it imperative for all parties involved to find a path toward de-escalation and peaceful resolution of the conflict.

BIBLIOGRAPHICAL REFERENCES:

1. Bachmann, S. (2022). *The Drone War in Ukraine: Tactical Advantages and Strategic Impact.* In *Journal of Modern Warfare Studies*, 5(2), pp. 132-147.
2. Bender, J. (2022). *Ukraine's Use of Bayraktar Drones Against Russian Forces*. In *Defense News*.
3. *Both sides in the Russia-Ukraine war are using new and old technologies for warfare*, 2024, https://theconversation.com/both-sides-in-the-russia-ukraine-war-are-using-new-and-old-technologies-for-warfare-225451, retrieved on 22 July 2024.

4. Carroll, J. (2022). *Eyes in the Sky: How Drones Are Changing the Dynamics of War.* In *Military Review.*
5. Conflict Monitoring Organizations (2023) – Data and reports from organizations tracking the Russia-Ukraine conflict, including drone use and cross-border incidents.
6. Defense Express (2023). *The Role of Loitering Munitions in Modern Warfare*: *Lessons from the Russia-Ukraine War.*
7. Dukowitz, Z. (2024), *Police Drones: A Guide to How Law Enforcement Uses Drones in Its Work,* https://uavcoach.com/police-drones, retrieved on 12 August 2024.
8. Global News Outlets (BBC, Reuters, Al Jazeera) (2023) – *News coverage and analysis of the Russia-Ukraine war, including attacks near the Romanian border and subsequent discoveries of drone debris*.
9. Grossman, D., (2022). *Electronic Warfare and Drones in the Russia-Ukraine War*. Military Technology Review.
10. Kamp, K. (2022). *The Impact of Bayraktar Drones on the Ukraine War*. War on the Rocks.
11. Komarov, I. (2023). *The Russian Drone Arsenal in Ukraine: Types, Capabilities, and Deployment*. In *Russian Military Journal*.
12. Kyiv Independent (2023). *Drone Warfare: Ukrainian Innovations in the Face of Russian Aggression.*
13. NATO Press Releases (2023) – NATO communications regarding incidents involving drones in Romanian territory and collective defence assurances.
14. Roblin, S. (2022*). How Effective Are Russian and Ukrainian Anti-Drone Countermeasures?* In *Forbes.*
15. Romanian Ministry of Defence Reports (2023) – *Various reports on the discovery of drone debris and Romania's responses.*
16. Schcherbak, S. (2024). *Ukrainian Drone Incinerates Russian Troops' Positions in Wooded Area,* https://en.defence-ua.com/news/ukrainian_drone_incinerates_russian_troops_positions_in_wooded_area_video-11724.html., retrieved on 22 July 2024.
17. Syngaivska, S. (2024). *Romania Confirms Russian Drone Entry into its Airspace, the F-16 Jets Have Been Dispatched,* https://en.defence-ua.com/news/romania_confirms_russian_drone_entry_into_its_airspace_the_f_16_jets_have_been_dispatched-11783.html., retrieved on 22 July 2024.
18. Sotoudehfar, S., Sarkin, J. (2024). *Drones on the Frontline: Charting the Use of Drones in the Russo-Ukrainian Conflict and How Their Use May Be Violating International Humanitarian Law,* ICLR, 2023, vol. 23, no. 2, https://www.researchgate.net/journal/International-and-Comparative-Law-Review-2464-6601, retrieved on 12 September 2024.
19. TASS (2023). *Russian Use of ZALA and Lancet Drones in Combat Operations*. TASS News Agency.
20. Ukrainian Military Updates (2023) – Statements and updates from Ukrainian military sources on Russian drone attacks near the Danube ports.

21. https://liveuamap.com/, retrieved on 12 August 2024.
22. https://newstrategycenter.ro/wp-content/uploads/2024/02/war_lessons_samus_short.pdf, retrieved on 12 August 2024.
23. https://www.icrc.org/sites/default/files/document/file_list/what-is-ihl-factsheet.pdf, retrieved on 12 July 2024.

NATIONAL STRATEGY – LINKAGE BETWEEN NATIONAL IDEAL AND NATIONAL INTERESTS –

Major General (ret.) Associate Professor Grudi ANGELOV, PhD

National Security Department, Faculty of Information Technologies, University of Library Studies and Information Technologies, Sofia

DOI: 10.55535/RMT.2024.4.34

The report examines the main factors, characteristics and elements of national power, the formulation of national interests and objectives, emphasizing the bridging role of national strategy. The national strategy articulates the ways to achieve national goals, where a connection is made with national power. Therefore, the article focuses on working definitions of national power and national strategy, as well as on the linkages between national power, national interests, and national strategy. In addition, the importance of defining the national interests and goals is depicted.

Keywords: national strategy; national ideal; goals; power; policy;

INTRODUCTION

Since the dawn of the 21st century, numerous conflicts have unfolded, including a recent one on European soil. The underlying causes of these conflicts and the resulting armed confrontations (wars) echo Clausewitz's definition, which states that: *"war is simply a continuation of political relations with the addition of other means"* (Clausewitz, 1976, p. 605). Later in the same chapter, Clausewitz emphasizes that *"we deliberately use the phrase <with the addition of other means> because we also want to make it clear that war does not in itself stop political communication or transform it into something entirely different"* (Ib.).

The conclusions to be drawn from these two quotes are that wars emerge as a consequence of pursuing political objectives within a strategic framework. In this framework, national interests are clearly articulated, national goals are explicitly defined, and the state's instruments of power and resources are identified and mobilized to achieve these objectives. National goals and interests are dynamic and continually evolving. Similarly, national power and security are intrinsically linked to these goals. Thus, it can be concluded that power serves both as a means to achieve national interests and as an end in itself.

An objective expression and primary manifestation of national power lies in the implementation of national strategy. Conversely, the strength and effectiveness of national power are significantly influenced by the quality of the national strategy.

To analyse the relationship between national strategy, national ideal, and national interests, a systemic approach has been employed. This approach uses a cyclical, reversed application of analytical and synthetic methods, relying on systemic decomposition and aggregation.

WORKING DEFINITIONS OF NATIONAL POWER, NATIONAL STRATEGY, NATIONAL IDEAL, NATIONAL INTEREST

National power, as a geopolitical concept, affects the mass characteristics of the state, which represent the sum of their capabilities and potential. There are many definitions of national power, but we will use only three of them that reveal the connection between national power and national interests:

- **National power** consists of the material and spiritual capabilities that exist in a geographical and political unit called a state or government (Hafeznia, 2003, p. 51);

- **National power** means the ability, potential, and capacity of a nation and state to use its material and spiritual resources to impose its will to achieve its national interests and goals (Shuofeng, 1992, p. 102);
- **National power** can be defined as the country's ability to pursue strategic goals through purposeful action.

Taking into account the above-mentioned aspects, national power could be viewed through two distinct but related dimensions: an external dimension, which consists of the nation's ability to influence the global environment through its economic, political, and military potential, and an internal dimension, which consists of the nation's ability to transform society's resources into actionable knowledge (Angelov, 2018, p. 87).

Strategy (Wikipedia.org, 2023), derived from the Greek term *στρατηγία, stratēgia*, meaning *"art of military leadership, office of military commander, command etc."*, refers to a high-level plan designed to achieve one or more objectives under conditions of uncertainty. Its importance stems from the limited availability of resources to achieve these goals. Strategy typically involves setting objectives, identifying actions required to accomplish them, and mobilizing the necessary resources. In essence, strategy outlines the approach to achieving final objectives by aligning actions with available resources. Similarly, in organizational studies, defining strategy is a key responsibility of management. A strategy may emerge as a template or model for activity. The process of creating a strategy involves complex practices such as strategic planning and strategic thinking.

Comparing the two definitions, it is evident that strategy shares several components with doctrine, such as establishing goals, determining methods to achieve them, and allocating resources. However, strategy is generally constrained by a specific timeframe and focuses on shorter-term objectives. Fundamentally, strategies serve as tools and approaches for realizing national interests and achieving overarching objectives. An example of this concept in practice is the *"Updated National Security Strategy"* adopted in 2018 (National Assembly of the Republic of Bulgaria, 2024).

The concept of strategy is neither straightforward nor universally understood. Over time, the term *"strategy"* has become a cliché, often used casually in everyday conversations and media to refer broadly to plans, concepts, courses of action, or visions across personal, organizational, and governmental levels. However, it lacks specificity in defining the conditions under which the strategic development process begins, the foundation for analysing the security environment, and how these factors influence the identification of national interests, policies, goals, and the means to achieve them.

Simply put, strategy at any level is a framework of goals, resources, and action plans within acceptable risk boundaries, designed to create more favourable outcomes than would naturally occur or might otherwise benefit third parties. One definition describes strategy as *"the art and science of developing and using instruments of national power to synchronize and integrate ways to achieve national and multinational goals"*. While both definitions offer valuable insights, neither of them fully encapsulates the role and complexity of strategic thinking at the highest levels of governance. Strategy strives for synergy and balance among goals, concepts and resources to enhance the likelihood of success in government policies and amplify the impact of that success.

Additionally, strategy serves as a comprehensive plan to connect the present with a desired future. At the state level, it involves employing specific instruments of power – diplomatic, economic, military and informational – to achieve political objectives, often in collaboration or competition with other actors pursuing potentially conflicting goals. In essence, strategy is the application of state power, leveraging natural and societal resources, to fulfil political aims within a dynamic and competitive strategic environment.

A foundational assumption of national strategy is that all nation-states and non-governmental organizations have interests they seek to advance. These interests represent desired end states, often categorized as survival, economic prosperity, a favourable global order, or enduring national or group values. Derived from these broad categories, interests are shaped by the strategic environment and can be further refined in relation to specific issues. The elements of national power serve as the resources used to safeguard or promote these interests.

The national ideal for every nation and state expresses its great, supreme goal, which represents a kind of connection between past, present and future. The ideal is a dynamic category reflecting specific historical goals and objectives. The same directs the focus of the nation to the unity of specific national values, which largely reveal the historical aspirations and the aspirations of the nation, as well as to forming the idea of its own vocation.

The national ideal, on the other hand, is also the basis of the nation's political philosophy and culture, which is the basis for forming and preserving national self-awareness. It is a unique reflection of various aspects of the nation's life and activities in political, military, economic, cultural and social terms. The same, in addition to the possessed quantitative and qualitative characteristics, in different historical periods were carriers of different weight coefficients.

National interests are a rapidly changing (dynamic) function of the national ideal. They represent the general need of the nation to express its rights and claims by referring to its historical development. They could refer to territories, population, cultural monuments, preservation of historical memory, as well as to everything related to increasing its spiritual and material condition. Expectations from the realization of national interests are the receipt of certain benefits.

National interests, on the other hand, are the ways to achieve the national ideal. They are the active component that, depending on changes in the security environment, can be modified and shaped over time. On the other hand, national interests are perhaps among the most significant functions of the national power of the modern state.

The concept of national interest has been used for many years by politicians and statesmen as the main criterion in assessing threats to the existence and prosperity of the nation in any crisis situation caused by geopolitical, regional and local changes, as well as in the analysis and evaluation of the appropriate actions by the state. The concept dates back for centuries and is associated, in particular, with the formation and development of the nation-state in the 16th and 17th centuries. Moreover, there have always been difficulties in reaching agreement on a precise definition of the concept of national interest. Even today, we have political and military leaders, diplomats, and scientists who talk about the *"national interest"* in the emergence of various international situations, without defining its meaning or under what exact criteria they have reached their conclusions. In this aspect, Professor Frankel finds acceptable the Brookings Institution's definition of *"national interest"* as *"the common and permanent ends for which a nation acts"* (Rosenau, 2006, p. 36).

ASPECTS OF NATIONAL IDEAL

The national ideal is, as mentioned, a reflection of the most representative aspects of the nation's life and activities as follows:

❖ **The political aspects** of the national ideal express the desire for the development of the nation, its unification and generation of sufficient national power to declare itself to the world as a country with sufficient power. Moreover, the national ideal is its basis for guaranteeing the national independence, territorial integrity and sovereignty of the state, as well as for the construction of an independent, sovereign and strong state. All this leads to an increase in the self-confidence of the nation, upgrading the dignity and pride of the citizens of the country, and subsequently, after the generation of sufficient power and self-confidence, to the increase in its international authority (Nejkova, 2022, p. 75);

❖ **The economic aspects** are an expression of the state's ambitions to ensure the well-being of every individual citizen by improving working and living conditions, increasing employment for more and more people. The increase in the national capital also leads to the so-called economic nationalism, which is a consequence of an increase in the national production and therefore the gross domestic product (GDP), which in turn leads to an increase in the competitiveness and quality of the goods and services offered;

❖ **Military aspects** reflect the country's national power and are a guarantor of the country's sovereignty and independence. At the same time, taking into account the complex geopolitical situation in the region and the world as a whole, it is necessary for any country to maintain armed forces capable of dealing with possible challenges dictated by the rapidly changing security environment and to *"guarantee the sovereignty, security and independence of the country and to protect its territorial integrity"* (Parliament, 2007);

❖ **Geopolitical aspects** are the basis of the national ideals of each and every nation. In such a context, nationalism is a democratic factor as well as a factor for establishing peace and regional security.

❖ **The cultural aspects** of the national ideal are a direct reflection of the desire for continuous development of the nation in spiritual and intellectual terms. Culture and education are among the fundamental factors for the formation and strengthening of national identity, as well as for its preservation. Therefore, efforts to increase the education and culture of the citizens of the state are of utmost importance for achieving the national ideal.

When formulating the national ideal, it is necessary to approach it extremely carefully, taking into account the distinctiveness of the era to which it refers, in order to determine the ways and means of its achievement. On the other hand, in order to accomplish this ideal, it is necessary for the leaders to be nationally responsible and to define and achieve the short- and long-term goals of the state, as well as to formulate national interests.

HISTORICAL APPROACH TO NATIONAL INTERESTS AND GOALS

From ancient times, national interests have determined relations between states in a given region or on a global scale. National interests are, as above-mentioned, a dynamic function of the national ideal, an active component that, depending on the changes in the security environment, can be modelled in time.

National goals and interests (Teodosiev, 2022) are not stagnant; therefore, they are active and changing. National power and national security are among

the national goals that state governments try to achieve with the tools used to increase national power. National interests are the main driving force of any nation and can be pointed for solving foreign and internal political issues.

Depending on their subject of action, national interests are rationally grouped as: political; economic; cultural; geopolitical etc. They must support the formulation of policies for implementing the set national goals. For example, the Bulgarian national interests from the liberation (1878) until today have not been developed correctly, systematically and consistently, in terms of not only their definition, development and formulation, but also their achievement. In the scientific development and formulation of national interests, it is necessary to pay particular attention to the historical development of issues of national importance (Zahariev, 2022) and to analyse the needs for solving these issues and the contributions they would bring to the nation after their realization. On the other hand, it is necessary to draw lessons not only from the successes and achievements, but also from the accumulated negative experience in their implementation. Our history is rich with such negative examples. These examples include those mistakes that have caused damage to the Bulgarian national cause. Today, we call many of them political absurdities leading to national catastrophe. They are political absurdities because they were formulated without deriving from the national ideal of Bulgaria and without defining the national goals. As mentioned above, national interests are the means of achieving the ideal of any country and therefore must be fully directed for its realization. In addition, the interests need to be derived from the national goals and therefore to be leading for the nation for a long period (at least twenty-five years).

National interests should describe how the state would fulfil its strategic goals, which should be open and extend beyond the country's territory. The focus of interests should not be directed to territorial claims to neighbouring countries or to the acquisition of foreign resources, but to maintaining national self-awareness of all citizens located outside the territory of the state. The main goal of every country should be the preservation of its national and cultural identities, the protection of the rights and interests of citizens, as well as the assistance in supporting the country in all international institutions.

When determining national interests, it is necessary to approach them with moderate realism, excluding the extremes leading to unjustified maximalism or to nihilism, which in turn can be extremely harmful. Therefore, a balance must be found between the important needs and the possible harmful consequences that would arise from their realization.

The determination and realization of national interests should not be subordinated to the political biases of one party or a coalition of parties, because over the years politicization and political extremes have often left a negative imprint on the determination and realization of national interests. Moreover, in the implementation of national interests, it is necessary to ensure continuity and consistency for their realization. In order to achieve it, national consent is needed, putting the interests of the nation before the interests of individual parties, factions and groups.

In order to determine whether the national interests are formulated correctly, it is necessary to create and use criteria. These criteria should support the work of the ruling political elite to determine:

- whether they contribute to the realization of the national ideal;
- their contribution to the protection of the freedom and independence of the nation and the state;
- the degree of risk for the state in the consistent defence of the formulated national interests.

Therefore, from everything that has been mentioned so far, it can be concluded that national interests are the main driving force of every nation and state. They are based on the national ideal and the national goals of the state, determining the national and state policy. The implementation of the same should be the primary (main) task of all political leaders, politicians and public figures, whose duty is to ensure the well-being of each individual citizen of the state, as well as the prosperity of the nation.

THE CONNECTIONS BETWEEN NATIONAL POWER, NATIONAL INTERESTS AND STRATEGY

National power has the rare ability to develop and expand continuously, provoking states to permanently generate more and more power and, accordingly, improve their place in the system of international relations. Therefore, it can be concluded that national power is active in nature. It can often be seen as a national goal and can be used as a tool to achieve national goals as well.

When formulating a national strategy, one of the most important things is the correct determination and definition of goals. All too often, strategy development does not take sufficient time to consider appropriate objectives in the context of desired policy, national interests, and the security environment.

National goals and interests are also active and constantly changing. National power and national security are among the national priorities that state governments

try to realize using levels of national power. Therefore, national power could be seen as both a goal and as a means of government to achieve national goals and interests.

The national security strategy is both an objective form and a basic manifestation of the application of national power. The national strategy, on the one hand, is a strategic document of the state for presenting the ways to achieve the most effective model of national power, and on the other hand, its implementation is directly dependent on the level of national power.

Talking about strategy, it could be said that, in general, it is defined by the art of the political leaders of a country to consider the capabilities, opportunities and level of national power, on the one hand, and the achievement of its national interests and goals, on the other hand. As a next step, they must define and adopt policies to achieve national goals and interests using the level of national power reached.

The main motive for increasing national power is the lack of resources, because *"the lack of sufficient available resources to achieve national goals activates the motivation to increase power to achieve these goals"* (Seifzadeh, 1997, p. 144).

CONCLUSIONS

In conclusion, it can be determined that national interests are gritty because of the assessment of the security environment (global and internal for the respective country). On the one hand, the assessment of national power is used to analyse the security environment and determine the place and role of the respective state in international relations and its influence internationally, as well as in the process of determining the desired end state (national interests and goals). On the other hand, the factors and elements of national power are also the means for realizing national interests and goals. Therefore, the national security strategy simultaneously uses the same for the assessment and analysis of the security environment, as well as for resource provision, the fulfilment of national interests. Moreover, it can be unconditionally concluded that strategy is the connecting link between national power and national interests.

Therefore, there is a threefold relationship between national power, national interests and national strategy. The quality of satisfying national interests depends on the level and quality of the national power of the country. To establish a relationship between these two variables, national interests and national power, strategy plays an important role as a link between these two phenomena – power and its instruments, on the one hand, and purpose, on the other hand. Therefore, it is assumed that strategy is the art of applying national power to achieve national goals (Ib., p. 302).

Acknowledgement and financin: This work was supported by the NSP SD program, which has received funding from the Ministry of Education and Science of the Republic of Bulgaria under the grant agreement no. Д01-74/19.05.2022.

BIBLIOGRAPHY:

1. Angelov, G. (2018). *Conceptual model of the system country-hood – security*. Sofia: Institute of research and development of PhD students, University of Library Studies and Information Technologies.
2. Clausewitz, C. V. (1976). *On War*. Indexed Edition. New Jersey: Princeton University Press, 1976, pp. 605, 735.
3. Hafeznia, M. (2003). *Analysis of geopolitical basis of national power of Islamic Republic of Iran*. Tarbiat: Tarbiat Moalem University Press.
4. National Assembly of the Republic of Bulgaria (2007). Конституция на Република България. Sofia: Siela-Soft End Publishing.
5. National Assembly of the Republic of Bulgaria (18 September 2024). Aktualizirana strategia za natsionalna sigurnost na, file:///C:/Users/User/Downloads/Aktualizirana_strategiya_za_natsionalna_sigurnost_na_Republika_Bulgaria_2018%20(1).pdf, retrieved on 6 October 2024.
6. Nejkova, M. (2022). *Grazhdanskoto obshtestvo- faktor na sigurnostta v darzhavata*. Sofia: Avangard Prima.
7. Rosenau, J. (2006). *Study of World Politics: Theoretical and Methodological Challenges*. Abingdon, Oxon OX14 4RN: Routledge Taylor &Francis Group.
8. Seifzadeh, H. (1997). *Theory-Building in International Relations Fundamentals and Paradigms* (13th ed.). Tehran, Iran: Samt publication. Retrieved on 18 September 2024.
9. Shuofeng, H. (1992). *Comprehensive National Power Studies*. Chinese Academy of Social Studies Press.
10. Teodosiev, P. (2022). *Savremenni diplomaticheski sposobi za uregulirane na konflikti i krizisni situatsii*. Pravo i Sigurnost. Burgas: Burgaski svoboden universitet.
11. Wikipedia.org. (26 June 2023), https://bg.wikipedia.org/wiki/%D0%A1%D1%82%D1%80%D0%B0%D1%82%D0%B5%D0%B3%D0%B8%D1%8F, retrieved on 18 September 2024.
12. Zahariev, A. (2022). *Aktualni vaprosi, otnosimi kam obuchenieto v profesionalno napravlenie nacionalna sigurnost*. Akademichni partnyorstva v sferata na natsionalnata sigurnost.

BRIDGING THE GAP BETWEEN ANALYSIS AND PREDICTION – TOWARDS THE DEVELOPMENT OF AN INTEGRATED PREDICTIVE MODEL FOR HYBRID THREAT RISK ASSESSMENT –

Colonel Professor Cezar VASILESCU, PhD Habil., BEng

Associate Professor Aura CODREANU, PhD

Regional Department for Defence Resources Management Studies (DRESMARA) Brașov;
"Carol I" National Defence University", Bucharest

DOI: 10.55535/RMT.2024.4.35

This article analyses the common patterns of recent hybrid threats, highlighting some representative cases such as: the information warfare during the US elections (2020), the COVID-19 vaccine disinformation campaign (2020-2021), and the energy crisis in Europe (2021-2022), in order to identify the existence of potential synergies between different tactics (cyber, information, economic) depending on the specific context. On the basis of these patterns, the article proposes the essential parameters of a predictive hybrid threat analysis model (including geopolitical, cyber, economic, social, media, political and technological factors) with the aim of facilitating proactive responses to this type of threats in modern society.

Keywords: hybrid threats; disinformation; modern conflicts; economic pressure; cyber-warfare operations;

INTRODUCTION

In recent decades, the international security environment has undergone major transformations, becoming increasingly complex and unpredictable. Today, it is defined by instability and uncertainty and is influenced by a number of global factors (rapid digitalization of society, interconnectedness of national economies, increased complexity and interconnectivity between states, intensified competition for strategic resources and geopolitical influence, and political volatility) that have led to new vulnerabilities that can be exploited by state and non-state actors.

The latter are continually adjusting the tactics they use to exploit these vulnerabilities, as the use of hybrid elements offers a significant advantage: relatively low cost, minimized risk, and less likelihood of generating a large-scale military response (Pindják, 2019). For example, the use of social media and other digital communication platforms has become an essential tool in influence and destabilization campaigns (Galeotti, 2019).

In this context, globally, hybrid threats have become a preferred tool to undermine the stability of states and regions. In contrast to conventional armed conflicts, these threats manifest themselves in multiple forms, involving a combination of tools and methods that cover the military, non-military, cyber and informational domains (Hoffman, 2007).

These hybrid threats combine multiple unconventional techniques and tactics (from cyber-attacks against critical infrastructures – such as health or energy – to disinformation campaigns and economic pressure) in an integrated and subtle way to weaken national stability without triggering a traditional military response. A common feature of these cases is the *use of synergy between several forms of aggression*, which complicates the process of detecting and countering them.

The concept of *"hybrid threat"* is not new, but its formal use in the security literature has grown exponentially over the last decade, particularly in the context of modern conflicts. Hybrid threats are defined as a combination of conventional and unconventional methods, including cyber-warfare operations, disinformation, economic attacks, and political and social influence tactics. According to a NATO report, hybrid threats are characterized by the *"Coordinated and synchronized use of different means and activities, aimed at exploiting vulnerabilities in societies and undermining the political and economic stability of target states"* (NATO, 2020).

They manifest themselves in a *"grey space"* of conflict, where it is difficult to distinguish between peace and war, and the responsible actors often remain undetected or officially unidentifiable (Mumford, 2021).

Also, Hoffman (2007) defines hybrid threats as *"A synthesis of conventional and unconventional methods, including terrorism, insurgency, and cyber warfare, which are combined into an integrated campaign".* Another definition of the concept of hybrid threats is offered by Rid and Hecker (2021). According to them, it represents *"operations that combine cyberattacks with other forms of aggression, including economic pressure and disinformation"*, while, as the same authors underline, their multisector dimension needs to be highlighted. The immediate consequence of integrating multiple domains is that responding to such threats becomes a difficult and challenging task.

One of the fundamental characteristics of hybrid threats is the use of a wide range of tactics in a synergistic manner. This approach allows actors to exploit vulnerabilities on multiple fronts simultaneously, thus creating multidimensional pressure on the target. Synergy between cyber, information and economic tactics has become a defining element in recent hybrid conflicts. For example, cyber-attacks can be coordinated with disinformation campaigns to amplify destabilizing effects, while economic pressures can be used to weaken the resilience of states.

According to studies by Wither (2016), the synergy of these threats is characterized by the integration and coordination of multiple domains (including cyber, information and economic). According to the aforementioned author, the essential element in defining a hybrid threat is that the vulnerabilities of a target state are taken advantage of, especially in the context of social, economic and political divisions. Thus, while the nature of the attacks may vary, their common aim is to destabilize order and weaken the response capabilities of the targets.

In this context, the fundamental assumption of the first part of this paper is that *"Hybrid threats use a combination of cyber, informational and economic tactics tailored to the specific context of each target state, and their success depends on the degree of integration and synchronization of these tactics, whose synergy amplifies the destabilizing impact"*.

To test this hypothesis, the current research will use comparative analysis as a method to review several recent cases of hybrid threats, selected on the basis of their geopolitical relevance and impact. By analysing these cases, we will proceed to *identify their individual specific patterns and, in the end, describe possible common patterns*. We will also analyse how different tactics (cyber, informational, economic) have been combined and coordinated to achieve the objectives of the actors involved.

This hypothesis assumes that hybrid tactics are not used in isolation, but synergistically (Otaiku, 2018), tailored to the specific vulnerabilities of each state, whether economic (such as sanctions or energy crises), informational (disinformation and propaganda campaigns), or cyber (attacks on critical infrastructure).

Among the main sources used in this analysis to test the validity of the underlying hypothesis are recent NATO (2020) report studies, as well as theoretical and empirical work on hybrid threats (Hoffman, 2007; Wither, 2016; Pindjak, 2014 and 2019; Galeotti, 2019; Rid, Hecker, 2021).

Ultimately, we will seek to demonstrate that achieving the objectives of these hybrid threats depends on coordination across multiple domains and tailoring tactics to the specific vulnerabilities of each target.

COMPARATIVE ANALYSIS OF HYBRID THREATS

The study of hybrid threats represents a major challenge for international security research, given their complexity and their ability to adapt rapidly to changes in the global security environment. By comparatively analysing several recent cases and identifying common patterns of action, this research aims to provide a better understanding of the mechanisms underlying these threats and to contribute to the development of effective countering strategies.

In the following paragraphs we will briefly examine each of the selected cases, using as analysis parameters the purpose, the tactics used, the vulnerabilities exploited and the patterns identified.

A. Information warfare during the US election (2020) (National Intelligence Council, 2021; Wojnowski, 2021; Menn, 2020).

- Purpose: Undermine confidence in the American electoral process and destabilize politics.
- Tactics used:
  - Disinformation and propaganda: massive spread of conspiracy theories and false information about electoral fraud.
  - Cyber-attacks: hacking attempts on electoral systems and critical infrastructure.
  - Exploiting social divisions: Amplifying racial and political tensions through fake social media accounts.
- Exploited vulnerabilities:
  - Political polarization: the deep divide between political parties and social groups in the USA.

- Low trust in public institutions: at an already low level it was amplified by disinformation campaigns.
- Social platform addiction: Vulnerabilities in social networks used to spread misinformation rapidly.

- Patterns identified:
  - Multi-modal coordination: the combined use of online (disinformation and cyber-attacks) and offline techniques – as a result of the former (protests and social tensions).
  - Long-term goals: creating an atmosphere of widespread distrust in democratic institutions.

B. COVID-19 vaccine misinformation campaign (2020-2021) (Tsiklauri, 2021; Suarez-Lledo et al., 2021; Stokel-Walker, 2024)

- Purpose: To weaken the global response to the pandemic and increase distrust in health authorities.
- Tactics used:
  - Spreading misinformation: false information about the effectiveness and safety of vaccines was amplified on social networks.
  - Exploiting fears and emotions: messages that exploited fear of the unknown and suspicion of governments and corporations.
  - Informal alliances: using alternative media channels and influencers to spread anti-vaccination messages.
- Exploited vulnerabilities:
  - Distrust in health authorities: fear and confusion over new virus and vaccines.
  - Uncontrolled access to information on social platforms: it allowed conspiracy theories to spread rapidly.
  - Fragmentation of the information ecosystem: access to alternative channels of information undermining scientific consensus.
- Patterns identified:
  - Information fragmentation: creating and feeding alternative information ecosystems that undermine scientific consensus.
  - Time as a critical factor: use of critical periods (start of vaccination campaign) to maximize negative impact.

C. Europe's energy crisis (2021-2022) (Gilbert et al., 2021; Popkostova, 2022; Gross et al., 2024)

- Purpose: To exert political pressure on Europe in order to influence the geopolitical and economic positions of member states.

- Tactics used:
  - Manipulating energy prices: deliberately cutting natural gas deliveries, thus creating an energy price crisis.
  - Economic pressures: threats of complete disruption of supplies amid political tensions.
  - Misinformation and media messaging: amplifying narratives blaming European governments for the energy crisis, thus dividing public opinion.
- Exploited vulnerabilities:
  - Energy dependence on Russia: European countries were vulnerable because of their dependence on Russian natural gas.
  - Economic structure and fragility of the energy sector: lack of immediate alternatives for energy supply.
  - Domestic political sensitivities: growing public discontent over high energy costs.
- Patterns identified:
  - Economic influence: using critical economic resources as a geopolitical weapon.
  - Synchronization of actions: coordination between different hybrid tactics (economic, informational) to maximize impact.

D. Cyber interference in the French election campaign (2017) (Vilmer et al., 2018; O'Connor et al., 2020; Ferrara, 2017)

- Purpose: To undermine the electoral process and influence the outcome of the presidential elections.
- Tactics used:
  - Cyber-attacks: hacking and publication of sensitive emails and documents of Emmanuel Macron's campaign team.
  - Disinformation: spreading false information and conspiracy theories on social networks and in the media in order to discredit the candidate favoured by the West.
  - Message amplification: using social media networks and fake accounts to amplify the impact of disinformation.
- Exploited vulnerabilities:
  - Poorly protected cyber infrastructure: political and campaign systems vulnerable to cyber-attacks.
  - Tense electoral period: the attacks were coordinated at key moments, when destabilization could have had the greatest impact.

- Rapid spread of disinformation online: effective use of social networks to amplify exfiltrated information.

- Patterns identified:
  - Concerted cyber-attacks: coordination between hacking and rapid dissemination of information to cause chaos before the vote.
  - Pre-election targeting: exploiting the sensitive period before elections to maximize the destabilizing impact.

E. Hybrid operations in Ukraine (2014-present) (Starodubtseva, 2021; Wentzell, 2021; Nübel, 2020)

- Purpose: To divide the territorial integrity of Ukraine and influence political decisions.
- Tactics used:
  - Unconventional military aggression: the use of unmarked troops, known as *"little green men"*, to seize control of Crimea.
  - Disinformation and propaganda: creating and disseminating narratives to justify intervention and generate confusion concerning the events.
  - Economic pressure: using Ukraine's dependence on Russian natural gas to exert political pressure.
- Exploited vulnerabilities:
  - Ethnic and political divisions: exploiting tensions between the pro-Russian eastern regions and the rest of Ukraine.
  - Energy dependence on Russia: Ukraine was vulnerable because of its dependence on Russian gas.
  - Military and political weaknesses: lack of military preparedness and non-existent internal political consensus in the face of aggression.
- Patterns identified:
  - Combined use of military and informational means: combining subtle military tactics with a powerful disinformation campaign to create ambiguity and prevent a unified international response.
  - Pressure on critical resources: using energy resources as economic leverage to influence the political decisions of the target state.

F. The migrant crisis in Europe (2015-2016) (Kuvekalović et al., 2017; Braghiroli et al., 2026; Karolewski et al., 2018)

- Purpose: Destabilization of European states by exacerbating the migration crisis and increasing social tensions.

- Tactics used:
  - Manipulating migration flows: facilitating or directing migrant flows towards European borders, using human trafficking networks and providing incentives.
  - Disinformation and media bias: spreading disinformation about the nature and reasons for the migration crisis, amplifying fears and social tensions in host countries.
  - Exploiting social vulnerabilities: fuelling xenophobic and anti-immigrant sentiments among the European population, thus dividing societies and putting pressure on local governments.
- Exploited vulnerabilities:
  - Lack of a common migration policy: Europe was vulnerable due to the lack of a unified mechanism to manage the migration crisis.
  - Social tensions and fear of immigration: exacerbation of xenophobia among European populations.
  - Exposure to misinformation: using media and social networks to amplify the perception of a major crisis.
- Patterns identified:
  - Exploiting humanitarian crises: using real humanitarian crises to destabilize target countries by creating social and political divisions.
  - Media amplification: using the media and social networks to amplify the perception of a crisis that is much worse than the reality, and thus intensifying public reactions.

G. The migrant crisis on the Polish-Belarusian border (2021) (Zdanowicz, 2023; Bodnar et al., 2023; Jędrzejczyk-Kuliniak, 2023)

- Purpose: Destabilize the European Union and create internal tensions by using migrants as an instrument of political pressure.
- Tactics used:
  - Forced migration: Belarus has orchestrated flows of migrants to EU borders, especially Poland, to create a humanitarian crisis and force a reaction.
  - Propaganda: using state-controlled media to blame the EU for the humanitarian crisis, while Belarus denied any involvement.
  - Coercive diplomacy: threat of escalation if political demands were not met, including sanctions against the Lukashenko regime.

- Exploited vulnerabilities:
  - Poorly controlled borders: the lack of a solid border control infrastructure on Poland's border with Belarus at that time.
  - Internal EU tensions: exploiting EU divergences on migration policy.
  - Slow reaction from the authorities: the EU has been slow to react to Belarus' manipulation of migration.
- Patterns identified:
  - Migration as a weapon of destabilization: using migrant flows to exert political pressure on a regional entity.
  - The combination of coercion and propaganda: amplification of an artificially created crisis through disinformation and propaganda campaigns.

H. Intervention in the Catalan independence referendum (2017) (Vakarchuk, 2020; Arcos, 2021; Barberà, 2020)

- Aim: Amplify regional divisions and weaken Spain's national unity.
- Tactics used:
  - Disinformation and manipulation: spreading narratives supporting Catalan independence and encouraging confrontation between the central government and separatists.
  - Cyber-attacks: sabotaging websites and digital infrastructure associated with the Spanish government to hamper the response to the political crisis.
  - Protests and social unrest: encouraging and organizing mass protests and civil disobedience actions to amplify social tensions.
- Exploited vulnerabilities:
  - Nationalist and regional tensions: the historical conflict between Catalonia and the Spanish central government.
  - Institutional weaknesses: the central government had difficulties in managing the crisis, which aggravated tensions.
  - Exposure to disinformation: exploiting nationalist narratives and disinformation campaigns to fuel protests.
- Patterns identified:
  - Exploiting regional political divisions: focus on regional nationalist tensions to destabilize the nation state.
  - Synergy between disinformation and social mobilization: combining disinformation with direct social action to create a major political crisis.

I. Intervention in the political crisis in Venezuela (2019) (Rouvinski, 2019; Aulia et al., 2024; Rozental et al., 2022)

- Purpose: To influence the political balance in favour of the government in Caracas, despite international opposition.
- Tactics used:
  - International disinformation: spreading narratives legitimizing Nicolás Maduro's government and delegitimizing the Western-backed opposition.
  - Economic intervention and sanctions: using economic resources and trade relations to support the regime in the face of international sanctions.
  - Alliances and military support: providing military and logistical support through external allies to maintain regime's control.
- Exploited vulnerabilities:
  - Fragile economy: the severe economic crisis in Venezuela has been fertile ground for manipulation and disinformation.
  - Political polarization: deep division between regime supporters and opposition.
  - International isolation: the regime has benefited from the support of some foreign states, thwarting international sanctions.
- Patterns identified:
  - Sanctions and economic countermeasures: use of economic means to counter sanctions and support regime stability.
  - Information War: a global disinformation campaign targeting not only the local public but also the international perception of the political crisis.

J. Hybrid threats in Venezuela (2019-present) (Cañizález et al., 2020; Beaton, 2021; Chaguaceda et al., 2023)

- Purpose: To maintain Nicolás Maduro's regime in power despite economic and political crisis and international pressure.
- Tactics used:
  - Internal repression: the use of security forces to suppress protests and neutralize political opposition.
  - Information control: restricting access to information through censorship, media control and limiting internet access.
  - Disinformation: spreading narratives blaming foreign powers for the economic and political crisis, strengthening domestic support.

- Exploited vulnerabilities:
  - Authoritarian political system: using repression and information control to stay in power.
  - Resource dependence: control over natural resources (oil) has allowed the regime to resist sanctions.
  - Weakness of the opposition: the fragmentation and lack of a strong opposition leader was exploited by the regime.
- Patterns identified:
  - Internal repression and information control: simultaneous use of force and censorship to maintain control over the population.
  - Disinformation to legitimize the regime: spreading disinformation to counter international criticism and mobilize domestic support.

K. Political crisis in Belarus (2020-present) (Hardy, 2022; Giannakopoulou, 2022; Astapova et al., 2022)

- Purpose: Maintain Alexander Lukashenko's regime in power despite internal and external pressure for change.
- Tactics used:
  - Repression and human rights violations: use of force against protesters and pro-democracy activists to suppress opposition movements.
  - Disinformation: propagation of narratives delegitimizing opposition movements and presenting the regime as the only stabilizing force.
  - External support: recourse to Russian support, including military and economic support, to keep the regime in power despite international sanctions.
- Exploited vulnerabilities:
  - Authoritarian system: Lukashenko used repression and disinformation to suppress opposition movements.
  - Dependence on Russia: Belarus' vulnerability to Russian economic and military influence.
  - Internal social tensions: exploiting fear of change among the conservative population.
- Patterns identified:
  - Internal repression combined with disinformation: the simultaneous use of brute force and disinformation to discourage opposition and maintain control.
  - External support for stability: dependence on the support of a strong ally to survive to international and domestic pressure.

L. China's influence in Southeast Asia (2020-present) (Schmidt, 2008; Pal, 2021; Ferchen et al., 2023)

- Purpose: Expand China's economic and political influence in the region and counter Western influence.
- Tactics used:
  - Coercive diplomacy: the use of economic levers, such as investment and debt, to exert political influence over Southeast Asian states.
  - Disinformation and propaganda: promoting pro-China narratives in the region through state-controlled media and social networks.
  - Aggressive maritime activities: expanding territorial claims in the South China Sea by building artificial islands and militarizing the area.
- Exploited vulnerabilities:
  - Economic dependence: Southeast Asian states are vulnerable due to Chinese debt and investment.
  - Territorial disputes: states in the region are vulnerable because of territorial disputes in the South China Sea.
  - Democratic weaknesses: weaker or authoritarian regimes are easily influenced by economic levers.
- Patterns identified:
  - Using economic power as a political weapon: using economic dependencies created through investment and borrowing to control the political decisions of other states.
  - Non-military and military aggression: combining economic tactics with military presence to dominate a strategic region and limit the influence of rivals.

M. Chinese interference in Taiwan's politics (2019-present) (Chang et al., 2021; Hung et al., 2022; Hartnett et al., 2021)

- Purpose: Undermine Taiwan's political independence and reduce international support for the government in Taipei.
- Tactics used:
  - Disinformation: spreading fake news and conspiracy theories to weaken Taiwanese citizens' trust in their government.
  - Cyber-attacks: attacks on government institutions and critical infrastructure in Taiwan to destabilize the political and economic system.
  - Economic pressure: restricting Taiwan's access to international markets and pressuring other states not to recognize Taiwanese sovereignty.

- Exploited vulnerabilities:
  - Economic dependence: Taiwan is vulnerable to economic pressure from China on its trading partners.
  - Diplomatic isolation: Taiwan has few international allies and is under constant pressure from China.
  - Internal political tensions: exploiting Taiwan's internal political divisions.
- Patterns identified:
  - Synergy between cyber-attacks and disinformation: the combined use of cyber-attacks and disinformation campaigns to destabilize a democratic regime.
  - Economic pressure targeting political isolation: using economic influence to limit international support for a target country.

N. Political and security crisis in Mali (2012-present) (Thurston et al., 2013; Cox et al., 2018; Maza et al., 2020)

- Purpose: Maintain power and control over natural resources by destabilizing the region and limiting the influence of the central government and international peacekeeping forces.
- Tactics used:
  - Insurgency and terrorism: jihadist groups use guerrilla tactics, bombings and kidnappings to destabilize the region.
  - Disinformation and propaganda: spreading extremist ideology through social networks and local channels, strengthening public support for insurgent groups.
  - Exploiting social vulnerabilities: Manipulating ethnic and religious tensions to undermine social cohesion and weaken government.
- Exploited vulnerabilities:
  - Weakness of the central government: the Malian government has not been able to control all regions of the country.
  - Ethnic and religious tensions: exploiting tribal and ethnic rivalries in Mali.
  - Presence of extremist groups: vulnerability to the influence of jihadist groups active in the region.
- Patterns identified:
  - Combining insurgency with disinformation: the synergy between field operations and online propaganda to recruit and legitimize violent actions.
  - Exploiting social divisions: using ethnic and religious conflicts to intensify instability and prevent effective centralized government.

O. Iran's cyber interference campaign (2018-present) (Spataro, 2019; Elswah et al., 2021; Lehto, 2022)

- Purpose: Undermine the political stability of enemies and gain strategic advantage through cyber-attacks and disinformation.
- Tactics used:
  - Cyber-attacks: Iran orchestrated attacks on critical infrastructure in the US and its allies, including energy networks and financial systems.
  - Intellectual property theft: the theft of sensitive data and intellectual property from critical industries to develop its own technological capabilities.
  - Disinformation campaigns: launch of online campaigns to spread pro-Iranian narratives and discredit Western governments.
- Exploited vulnerabilities:
  - Unprotected critical infrastructure: cyber systems in the US and other allied countries were exposed to cyberattacks.
  - Poorly protected intellectual property: Iran exploited unprotected systems to steal critical data.
  - Negative perception of Western governments: amplifying anti-Western narratives.
- Patterns identified:
  - Strategic cyber aggression: the persistent use of cyber-attacks to destabilize adversaries and gain economic and military advantage.
  - Disinformation in support of cyber-attacks: spreading disinformation to amplify the effects of cyber-attacks and create confusion among the target population.

P. Russian influence in the Western Balkans (2014-present) (Lika, 2021; Cipan et al., 2024; Kase, 2024)

- Aim: To prevent the integration of Western Balkan states into the EU and NATO and maintain the Russian sphere of influence in the region.
- Tactics used:
  - Supporting pro-Russian parties: financial and logistical support to pro-Russian political parties and movements to influence national policies.
  - Disinformation: spreading disinformation to delegitimize the European Union and NATO while promoting pro-Russian narratives.
  - Ethnic and religious tensions: Exploiting ethnic and religious sensitivities to create instability and impede regional cooperation.

- Exploited vulnerabilities:
  - Political instability: the Balkan regions have been marked by simmering ethnic and political conflicts.
  - Energy dependence: Balkan states depend on Russian natural gas.
  - Economic weakness and corruption: exploiting poverty and corruption to gain influence.
- Patterns identified:
  - Political influence through financial support: use of material support to directly influence the domestic policies of target states.
  - Exacerbating social divisions: using historical and ethnic tensions to prevent European integration and destabilize the region.

*

The analysis of these cases allows highlighting some common patterns in the use of hybrid threats, which underline their complex nature, as follows:

- **Synergy between different fields of action:** In all the cases analysed, several types of actions/tactics (cyber, informational, economic) were combined to create multidimensional pressure on adversaries and to achieve the proposed objectives. This synergy is essential for the effectiveness of a hybrid threat.
- **Exploitation and manipulation of existing social and/or political crises:** Whether political, economic or territorial, social and psychological vulnerabilities (such as fear, political divisions or distrust of institutions) have been exploited to destabilize target states.
- **Propaganda and disinformation as a key tactic:** Propaganda and disinformation have been widely used to shape public perceptions and legitimize questionable international actions. Control and manipulation of information were key to influencing perceptions and destabilizing society.
- **Flexibility and adaptability**: The cases analysed demonstrated the ability of actors behind hybrid threats to adapt quickly to changing situations, using different means depending on the specific context (e.g. the rise of cyber-attacks during an election campaign or the manipulation of the energy market in the context of a political crisis).
- **Long-term influence**: Most of the hybrid actions analysed were designed to have long-term effects, aimed at gradually destabilizing trust in international institutions and alliances.

*

With regard to the hybrid tactics used, we note that they were not used in isolation, but in synergy. Thus, in *table 1*, we summarize them in order to identify how they were combined and coordinated to achieve the objectives of the actors involved and the type of synergy applied.

Table 1: Hybrid tactics used for each case analysed (authors' design)

Hybrid threat	Tactics used			Synergy type
	Cyber (C)	Information (I)	Economic (E)	
Information war during the US elections (2020)	Cyber-attacks on electoral infrastructure	Disinformation and propaganda campaigns	-	C-I
Disinformation campaign against COVID-19 vaccines (2020-2021)	-	Disinformation and propaganda on the effectiveness and safety of vaccines through anti-vaccination messages	-	I
Europe's energy crisis (2021-2022)	-	Disinformation and media messages blaming European governments	Energy price manipulation and economic pressures	I-E
Cyber interference in the French election campaign (2017)	Cyber-attacks on Macron campaign team	Disinformation and propaganda	-	C-I
Hybrid operations in Ukraine (2014-present)	Cyber-attacks on government infrastructure	Disinformation and propaganda	Economic pressures on energy resources	C-I-E

Hybrid threat	Tactics used			Synergy type
	Cyber (C)	Information (I)	Economic (E)	
The migrant crisis in Europe (2015-2016)	-	Migration crisis misinformation	Manipulating migration flows to create economic and social pressures	I-E
Migrant crisis on the Polish-Belarusian border (2021)	-	Anti-EU propaganda	Forced migration as political pressure	I-E
Intervention in the Catalan independence referendum (2017)	Cyber-attacks on government infrastructure	Disinformation and manipulation	-	C-I
Intervention in the political crisis in Venezuela (2019)	-	International disinformation	Economic interventions and sanctions	I-E
Hybrid threats in Venezuela (2019-present)	-	Internal disinformation to strengthen the regime	Economic pressure and internal repression	I-E
Political crisis in Belarus (2020-present)	-	Disinformation and propaganda to delegitimize the opposition	Economic and military support from Russia	I-E
China's influence in Southeast Asia (2020-present)	-	Regional disinformation and propaganda	Economic coercive diplomacy	I-E

Hybrid threat	Tactics used			Synergy type
	Cyber (C)	Information (I)	Economic (E)	
China's interference in Taiwan's politics (2019-present)	Cyber-attacks on institutions in Taiwan	Disinformation	Economic pressure on Taiwan	C-I-E
Political and security crisis in Mali (2012-present)	-	Jihadist disinformation and propaganda	Exploitation of natural resources and social tensions	I-E
Iran's cyber interference campaign (2018-present)	Cyber-attacks and intellectual property theft	Disinformation campaigns	-	C-I
Russia's influence in the Western Balkans (2014-present)	-	Disinformation to exacerbate ethnic tensions	Economic and logistical support for pro-Russian parties	I-E

We will also graphically present *table 1* in the form of a *"heat map"* diagram, which will represent the presence or absence of specific tactics for all 16 hybrid threats (a to p) in a two-dimensional way. This new representation allows a more intuitive analysis of the prevalence of each tactic within the hybrid threats and facilitates the rapid identification of patterns and trends in the use of these tactics.

In this representation:

- Each column represents a hybrid threat from the table above, labelled with the corresponding letter (a-p).
- The rows represent the three types of tactics: C (Cyber), I (Information), E (Economic).
- Red cells indicate the presence of a tactic for a particular threat.
- White cells indicate no tactic.

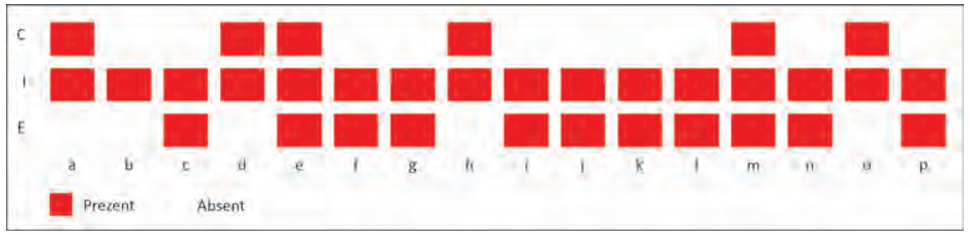


Figure 1: Hybrid tactics used for each hybrid threat.
(Heat map diagram) (authors' design)

Henceforth, based on the two graphical representations, we present a number of observations. Regarding the use of combined tactics, we observe the presence of C-I (cyber and informational only) in 3 cases, I-E (informational and economic only) in 8 cases, C-I-E (all three tactics) in 3 cases and I (informational only) in one case. The informational tactic (I) is also the most frequently used, forming an almost continuous line of red cells, and is applied in almost all but one case. This emphasizes the crucial importance of the informational component in hybrid threats.

Cyber tactics (C) are less common (occurring in only 6 out of 16 cases) and occur in combination with informational tactics in several cases. This suggests that, although important, cyber-attacks are not always a universal component of hybrid threats. Economic (E) tactics are present in about half of the threats, often in combination with informational tactics, forming an alternating pattern. This suggests that economic pressure is a significant but not universal component of hybrid threats. Last but not least, there are a few threats that use all three types of tactics (the fully red rows).

It becomes evident that information tactics play a central role in all hybrid threats, while economic and cyber tactics are used selectively depending on the specific nature of the threat.

As regards the hypothesis that hybrid tactics were tailored to the specific vulnerabilities of each individual target state/entity, *table 2* substantiates such a conclusion.

Table 2: Adaptation of tactics used in hybrid threats to the vulnerabilities characteristic of the cases analysed (authors' design)

Hybrid threat	Vulnerabilities	How to adapt tactics
Information war during the US elections (2020)	Political polarization, low trust in media, massive use of social networks	Disinformation exploited political divisions and racial tensions, while cyber-attacks targeted election infrastructure

Hybrid threat	Vulnerabilities	How to adapt tactics
Disinformation campaign against COVID-19 vaccines (2020-2021)	Lack of accurate information about vaccines, mistrust in authorities and medical institutions	Disinformation messages targeted reluctant groups and used social media to amplify mistrust
Europe's energy crisis (2021-2022)	Energy dependence on Russia, European market vulnerable to price fluctuations	Russia's cutting of gas supplies was used as an economic weapon along with disinformation to amplify public discontent with governments
Cyber interference in the French election campaign (2017)	Fragmented political system, strong social media presence in campaigns	Cyber-attacks and leaks targeting Macron's team accompanied by disinformation campaigns
Hybrid operations in Ukraine (2014-present)	Ethnic and linguistic divisions, economic instability and corruption	Russia has combined propaganda, unofficial military support and cyber-attacks to destabilize the country
Europe's migrant crisis (2015-2016)	Overburdened immigration system, rise of populist anti-immigration parties	Misinformation has heightened fears about immigration and manipulation of migrant flows has created economic and social pressures
Migrant crisis on the Polish-Belarusian border (2021)	Geopolitical tensions between EU and Belarus, anti-immigration rhetoric in Eastern Europe	Belarus used migration as political pressure and propaganda to divide EU countries
Intervention in the Catalan independence referendum (2017)	Regional tensions between Spanish government and Catalan authorities	Disinformation campaigns amplified separatist-propagandist narratives and cyber-attacks aimed to destabilize the government

Hybrid threat	Vulnerabilities	How to adapt tactics
Intervention in the political crisis in Venezuela (2019)	Collapsing economy, political instability, lack of popular support for Maduro	Economic tactics included international sanctions and disinformation to manipulate international opinion
Hybrid threats in Venezuela (2019-present)	Dysfunctional economy, tight government control over institutions and media	Disinformation was used for internal control and economic sanctions were used to weaken the economy and the opposition
Political crisis in Belarus (2020-present)	Lack of a well-organized opposition, external support from Russia	Disinformation has been used to discredit the protests and Russian support has strengthened the regime
China's influence in Southeast Asia (2020-present)	Economic dependence on China, territorial disputes in the South China Sea	China has used economic coercive diplomacy and propaganda to control regional states
China's interference in Taiwan's politics (2019-present)	Taiwan's limited international recognition, economic dependence on China	China has stepped up economic pressure and cyber-attacks on Taiwan, accompanied by disinformation
Political and security crisis in Mali (2012-present)	Political instability, presence of jihadist groups, dependence on international aid	Jihadists used disinformation for recruitment and exploited social tensions by manipulating access to natural resources
Iran's cyber interference campaign (2018-present)	Geopolitical tensions, severe economic sanctions, vulnerable cyber infrastructure	Iran deployed sophisticated cyber-attacks and disinformation campaigns to destabilize its external adversaries
Russia's influence in the Western Balkans (2014-present)	Ethnic tensions, political instability, low EU economic interest	Russia used propaganda to exacerbate ethnic tensions and logistical support for pro-Russian parties in the region

These cases show that each state was vulnerable to certain types of hybrid tactics, and the actors involved adapted their actions to the local context and specific weaknesses.

In conclusion, the study of these cases allows to formulate a recommendation on the need for an integrated and proactive approach to counter the sophisticated strategies of modern hybrid threats. It also emphasizes the need and importance of multidisciplinary monitoring, as authorities and experts need to constantly monitor a wide range of factors (from cyber activities to media narratives) in order to detect and respond effectively to hybrid threats. In terms of response strategies, it is essential to develop countermeasures that are as synergistic and interconnected as adversaries' hybrid tactics, combining cyber security, public communication strategies and economic resilience.

PARAMETERS OF A POSSIBLE INTEGRATED PREDICTIVE MODEL FOR HYBRID THREAT RISK ASSESSMENT

The implementation of a predictive model for hybrid threat analysis requires an integrated methodological approach able to combine and correlate variables from multiple domains (Valenza et al., 2022). The model needs to function as an adaptive mechanism that evolves with changes in the international security, economic and technological environment, thus enabling the anticipation and early detection of potential hybrid attacks. At the same time, it is generally accepted that *"Hybrid threats are traditionally difficult to anticipate ... but it is essential to analyse them in order to execute responses in a timely manner"* (Bertolini et al., 2023).

In a predictive hybrid threat analysis, the model used must be based on a set of essential parameters that reflect both the current context and previously identified patterns. These parameters are essential for creating a comprehensive situational awareness and for assessing the likelihood of a hybrid threat and its impact. Taking into account the typology of tactics described above, as well as the fact that *"Geopolitical cyberspace issues are closely linked to political, economic, social and cultural considerations"* (Douzet, 2014), we believe that such a model should include parameters that can be grouped into the following categories: ***geopolitical, cyber, economic, socio-cultural, media and informational, political*** and ***technological***.

We present in the following paragraphs the main parameters that we believe should be included in such a model, as well as details on the content of each of them, as follows.

A. Geopolitical parameters

These can be described by a set of specific sub-indicators, such as ***international tensions*** (the level of tension between states or regional blocs – e.g. latent conflicts, economic sanctions, territorial competition), the ***stability and cohesion of international alliances and agreements*** (NATO or the EU, and the effect of possible

ruptures on regional security), ***changes in national politics*** (legislative or policy changes that could influence a state's position on the international stage: elections, changes of government or economic policies that may provoke international reactions) and ***humanitarian/social crises*** (humanitarian crisis situations, mass migrations or internal social tensions that may be exploited by hybrid actors for societal destabilization).

B. Cyber parameters

They can be described by a set of specific sub-indicators, such as the ***volume and nature of cyber-attacks*** (the frequency and type of cyber-attacks – phishing, ransomware or DDoS attacks – detected against a specific target), ***known cyber-vulnerabilities*** (the level of exposure of critical infrastructure to cyber-attacks, including lack of software updates, unauthorized access or weak security practices), ***cyber capabilities of the actors involved*** (associated indicators ensue from the assessment of technical capabilities and resources available to known hybrid actors – nation states or cyber groups – that could launch an attack).

C. Economic parameters

These can be described by a set of specific sub-indicators, such as ***economic dependence on critical resources*** (economic vulnerabilities related to dependence on certain resources or suppliers – energy and raw materials, which could be leveraged in hybrid strategies), ***economic fluctuations and crises*** (economic indicators such as inflation, currency fluctuations, stock market declines or financial crises that can be exploited by hybrid actors for destabilization), and ***economic sanctions and trade*** (the impact of international sanctions or trade restrictions on a country or region and the way they could amplify existing economic vulnerabilities).

D. Social and cultural parameters

Those can be described by a set of specific sub-indicators, such as ***social divisions*** (the degree of social and political polarization, ethnic or religious tensions and other forms of fragmentation that can be exploited by disinformation and propaganda), ***public sentiment and trust in institutions*** (population's level of trust in government institutions, media and other key institutions – declining trust may facilitate hybrid disinformation actions), and ***social media activity and influence*** (monitoring dominant narratives on social networks and identifying disinformation or coordinated influence campaigns).

E. Media and information parameters

For this indicator, the set of specific sub-indicators can include the ***spread of disinformation*** (the frequency and extent of identified disinformation campaigns

and the types of narratives used to manipulate public opinion), ***media control and manipulation*** (the degree of control over the media and influence over the public agenda, including tactics to amplify messages through alternative channels and fake accounts) and ***public resilience*** (the level of media literacy and public resilience to disinformation, which influences the effectiveness of hybrid information campaigns).

F. Policy Parameters

These can be described by a set of specific sub-indicators, such as ***internal political stability*** (internal stability and unity of government, risk of revolts or opposition movements that could be encouraged by external actors), ***national security policies*** (effectiveness of security policies and the ability of the state to respond to hybrid threats through institutions such as the military, police and intelligence services), ***relations with external actors*** (level of cooperation or conflict with other states that may influence the likelihood of external hybrid action, and strategic alliances).

G. Technological parameters

For this indicator, the set of specific sub-indicators may include ***access to advanced technologies*** (the ability of actors to access advanced technologies – artificial intelligence, drones and advanced encryption that can be used in hybrid operations), ***innovations in communications and media*** (the role of emerging technologies in facilitating or countering hybrid campaigns, including the use of decentralized platforms or encrypted messaging applications).

CONCLUSIONS

Based on these parameters and the sets of specific sub-indicators identified, a predictive model can be built to provide a risk assessment for various hybrid threat scenarios. This paper aims only to suggest how it can be implemented and the essential elements to be considered, leaving further aspects for future research.

For this model to be functional, a fundamental aspect is the continuous collection and integration of data from various sources. According to Shan et al. (2024*) "A predictive analytics mechanism, integrated with threat intelligence platforms, utilizes historical data and current trends to forecast which attack vectors and potential targets are likely".* Ideally, implementation begins by building a data infrastructure that gathers information from a variety of relevant sources: geopolitical reports, real-time economic data, cybersecurity analytics, and social data (including analytics based on social network intelligence). This data infrastructure can be supported by a centralized system capable of harmonizing and constantly updating datasets in a dynamic way, reflecting recent developments.

A key element in this process is machine learning algorithms, which give the model the ability to identify patterns in historical and contemporary datasets. By training the algorithms with data from past hybrid scenarios (both successful and unsuccessful), a model can be built that detects correlations between different risk factors. These factors are found in geopolitical, cyber, economic, political and informational parameters, which together form the structure of a hybrid attack. For example, sudden changes in international relations or geopolitical tensions, combined with increased cyber activity in a particular region, can be early indicators of a coordinated hybrid attack.

Another key aspect is how the data is analysed to simulate potential scenarios. The model should be able to generate multiple simulations exploring different directions of hybrid threat evolution based on changes in geopolitical or economic parameters. These simulations can consider not only an isolated event, but also the synergy between different tactics commonly used in hybrid attacks: cyber-attacks combined with disinformation campaigns or the use of economic pressures to destabilize vulnerable targets.

For this model to be successfully implemented, an early warning system must also be developed. It should be programmed to trigger automatic alerts when the combination of factors reaches certain critical thresholds. For example, a rise in social tensions combined with an increase in cyber-attacks and disinformation campaigns may suggest that a hybrid crisis is imminent. Critical thresholds should be defined based on the analysis of past scenarios, and constant adjustments should be built into the system as new information becomes available.

Another important dimension in implementation is the resilience component. Once the model identifies a possible threat, it is important that the responsible authorities have a set of proactive measures in place, including building cyber resilience, implementing campaigns to increase public trust in national and international institutions, and working with international partners to counter the effects of hybrid threats in a coordinated manner.

In this way, the predictive model has the potential to become an essential tool for political and military decision-makers to plan their resources to prevent and mitigate the impact of hybrid threats before they cause significant damage. With a flexible structure and constant updating of data, the model can provide a comprehensive framework for anticipating threats, mitigating risks, and enhancing the safety of critical infrastructure and national security.

BIBLIOGRAPHY:

1. Arcos, R. (2021). *Information influencing in the Catalan illegal referendum and beyond*. In: Hybrid Warfare. DOI:10.5040/9781788317795.0023.
2. Astapova, A., Navumau, V., Nizhnikau, R., Polishchuk, L. (2022). *Authoritarian co-optation of civil society: The case of Belarus*. Europe-Asia Studies, 74(1), pp. 1-30.
3. Aulia, J.D., Kurniati, E. (2024). *Analysis of Russian factors supporting Nicolas Maduro in the Venezuelan crisis from Alexander Wendt's constructivist perspective.* Siyar Journal, 4(1), pp. 59-73, https://jurnalfisip.uinsa.ac.id/index.php/siyar/article/download/584/334, retrieved on 12 June 2024.
4. Barberà, O. (2020). *All fake? Information disorders and the 2017 referendum in Catalonia*. In Misinformation in Referenda (pp. 281-298). Routledge.
5. Beaton, A.C. (2021). *Social Media in Venezuela: A Tool for Authoritarians, a Boost to Social Movements, or Both?* Doctoral dissertation, Monterey, CA; Naval Postgraduate School, https://apps.dtic.mil/sti/trecms/pdf/AD1164874.pdf, retrieved on 12 August 2024.
6. Bertolini, M., Minicozzi, R., Sweijs, T. (April 2023). *Ten Guidelines for Dealing with Hybrid Threats. A Policy Response Framework*. The Hague Centre for Strategic Studies, https://hcss.nl/wp-content/uploads/2023/04/Guidelines-for-the-Deterrence-of-Hybrid-Threats-HCSS-2023.pdf, retrieved on 17 June 2024.
7. Bodnar, A., Grzelak, A. (2023). *The Polish–Belarusian border crisis and the (lack of) European Union response*. Białostockie Studia Prawnicze, 28(1), pp. 57-86, https://intapi.sciendo.com/pdf/10.15290/bsp.2023.28.01.04, retrieved on 17 June 2024.
8. Braghiroli, S., Makarychev, A. (2018). *Redefining Europe: Russia and the 2015 refugee crisis.* Geopolitics, 23(4), pp. 823-848
9. Cañizález, A., Hernández, L., Torrealba, L. (2020). *Disinformation as a Society-Wide Threat: Journalism and 'Fakecracy' in Venezuela*. In *Fake news is bad news – hoaxes, half-truths and the nature of today's journalism*, https://www.intechopen.com/chapters/73501, retrieved on 12 May 2024.
10. Chaguaceda, A., Pelaez, J.C., Puerta, M.I. (2023). *Illiberal Narratives in Latin America: Russian and Allied Media as Vehicles of Autocratic Cooperation*. Journal of Illiberalism Studies, vol. 3, no. 2 (2023): pp. 111-123.
11. Chang, H.C H., Haider, S., Ferrara, E. (2021). *Digital civic participation and misinformation during the 2020 Taiwanese presidential election*. Media and Communication, vol. 9, no. 1, pp. 144-157, DOI: 10.17645/mac. v9i1.3405, retrieved on 12 May 2024.
12. Cipan, V., Kirichenko, D. (2024). *Russian influence and disinformation operations in the Balkans*. Georgetown Security Studies Review, vol. 11, no. 2, pp. 65-85.
13. Cox, K., Marcellino, W., Bellasio, J., Ward, A., Galai, K.&Meranto, S., Paoli, G. P. (2018). *Social media in Africa*. *A double-edged sword for security and development.* RAND Europe, https://www.undp.org/sites/g/files/zskgke326/files/migration/africa/UNDP-RAND-Social-Media-Africa-Research-Report_final_3-Oct.pdf, retrieved on 22 May 2024.
14. Douzet, F. (2014). *Understanding cyberspace with geopolitics*. Hérodote, 2014/1, no. 152-153, pp. 3-21, https://shs.cairn.info/journal-herodote-2014-1-page-3?lang=en, retrieved on 17 June 2024.

15. Elswah, M., Alimardani, M. (2021). *Propaganda chimera: Unpacking the Iranian perception information operations in the Arab world*. Open Information Science, 5(1), pp. 163-174.
16. Ferchen, M., Mattlin, M. (2023). *Five modes of China's economic influence: Rethinking Chinese economic statecraft*. The Pacific Review, 36(5), pp. 978-1004, https://www.tandfonline.com/doi/pdf/10.1080/09512748.2023.2200029, retrieved on 22 May 2024.
17. Ferrara, E. (2017). *Disinformation and social bot operations in the run up to the 2017 French presidential election*, SSRN First Monday 22(8), http://dx.doi.org/10.2139/ssrn.2995809, retrieved on 22 May 2024.
18. Galeotti, M. (2019). *Russian political war: moving beyond the hybrid*. Routledge.
19. Giannakopoulou, S. (2022). *How social media mobilize the social and political reaction in authoritarian regimes: The Belarus experience*. Faculty of Economic and Political Sciences, https://ikee.lib.auth.gr/record/341645/files/GRI-2022-36486.pdf, retrieved on 13 June 2024.
20. Gilbert, A., Bazilian, M.D., Gross, S. (2021). *The emerging global natural gas market and the energy crisis of 2021-2022*. Foreign Policy, Brookings, 1, pp. 1-10, https://www.brookings.edu/wp-content/uploads/2021/12/FP_20211214_global_energy_crisis_gilbert_bazilian_gross.pdf, retrieved on 22 May 2024.
21. Gross, S., Stelzenmüller, C. (18 June 2024). *Europe's messy Russian gas divorce*, Brookings Institution, https://www.brookings.edu/articles/europes-messy-russian-gas-divorce/, retrieved on 22 August 2024.
22. Hardy, J. (2022). *Moving the goalposts: A Comparative case study analysis of the Belarusian regime*. Sciences, 10(9), pp. 100-107.
23. Hartnett, S.J., Su, C. (2021). *Hacking, debating, and renewing democracy in Taiwan in the age of "post-truth" communication*. Taiwan Journal of Democracy, 17(1), pp. 21-43.
24. Hoffman, F. (2007). *Conflict in the 21st Century: The rise of hybrid wars*. Potomac Institute for Policy Studies.
25. Hung, T.C., Hung, T.W. (2022). *How China's cognitive warfare works: A frontline perspective of Taiwan's anti-disinformation wars*. Journal of Global Security Studies, 7(4), pp. 1-18, https://doi.org/10.1093/jogss/ogac016, retrieved on 22 June 2024.
26. Jędrzejczyk-Kuliniak, K. (2023). *Polish-Belarus Border in the Political Narrative During the Migration Crisis in 2021-2022*, in Producing Cultural Change in Political Communities: The Impact of Populism and Extremism on the International Security Environment (pp. 159-181). Cham: Springer Nature Switzerland.
27. Kase, L.M. (2024). *The European Case for Kosovo, Serbia, and North Macedonia: A Western Balkan Focus*, https://digitalcommons.liberty.edu/cgi/viewcontent.cgi?article=1461&context=hsgconference, retrieved on 22 August 2024.
28. Karolewski, I.P., Benedikter, R. (2018). *Europe's refugee and migrant crisis: Political responses to asymmetrical pressures*. Politique européenne, (2), pp. 98-132, https://shs.cairn.info/revue-politique-europeenne-2018-2-page-98?lang=fr, retrieved on 22 May 2024.
29. Kuvekalović, J., Stojanović, G., Filipović, M. (2017). *Security implications of the migrant crisis in Europe 2015-2016*, Faculty of Security Studies.

30. Lehto, M. (2022). *Cyber-attacks against critical infrastructure.* In Cyber security: Critical infrastructure protection (pp. 3-42). Springer International Publishing. Methods in Applied Sciences, 56, https://doi.org/10.1007/978-3-030-91293-2_1, retrieved on 22 May 2024.
31. Lika, L. (2021). *The Western Balkans at the crossroads of European integration and the emerging powers' projection of influence*. The Journal of Cross-Regional Dialogues, no. 2/2021, pp. 7-30, https://orbi.uliege.be/bitstream/2268/265217/1/Article%20Liridon%20Lika%20JCRD.pdf, retrieved on 22 May 2024.
32. Maza, K.D., Koldas, U., Aksit, S. (2020). *Challenges of countering terrorist recruitment in the Lake Chad region: The case of Boko Haram.* Religions, 11(2), p. 96.
33. Menn, J. (2020). *Russian-backed organizations amplifying QAnon conspiracy theories, researchers say*, Reuters, https://www.reuters.com/article/us-usa-election-qanon-russia-idUSKBN25K13T, retrieved on 12 May 2024.
34. Mumford, A. (2021). *Hybrid Warfare: Past, Present, and Future*. Polity Press.
35. National Intelligence Council (10 March 2021). Foreign Threats to the 2020 US Federal Elections, https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf, retrieved on 22 May 2024.
36. NATO (2010). *A hybrid warfare strategy*. NATO Review.
37. NATO (2020). *NATO's Approach to countering hybrid warfare*. NATO Strategic Communications Centre of Excellence.
38. Nübel, K. A. (2020). *THE rise of new types of war: A case study on Russian hybrid warfare in the Ukrainian crisis in 2014*, Master's thesis, University of Twente, https://essay.utwente.nl/82683/1/N%C3%BCbel_MA_BMS.pdf, retrieved on 22 May 2024.
39. O'Connor, S., Hanson, F., Currey, E., Beattie, T. (2020). *Cyber-enabled foreign interference in elections and referendums* (vol. 28). Canberra: Australian Strategic Policy Institute, https://ad-aspi.s3.amazonaws.com/2020-10/Cyber%20enabled%20foreign%20interference_0.pdf, retrieved on 22 May 2024.
40. Otaiku, A.A. (2018). *A framework for hybrid warfare: threats, challenges and solutions*. Journal of Defense Management, https://www.longdom.org/open-access/a-framework-for-hybrid-warfare-threats-challenges-and-solutions-25432.html, retrieved on 22 May 2024.
41. Pal, D. (2021). *China's influence in south Asia. Carnegie Endowment for International Peace*, https://carnegie-production-assets.s3.amazonaws.com/static/files/202110-Pal_SouthAsiaChina_final1.pdf, retrieved on 22 May 2024.
42. Pindjak, P. (2014). *Deterring hybrid warfare: A NATO Perspective*. NATO Defense College Research Paper, 123, pp. 1-8.
43. Pindják, P. (2019). *The Hybrid threat: Blurring the line between war and peace*. Journal of Strategic Studies, 42(3-4), pp. 271-292.
44. Popkostova, Y. (2022). *Europe's energy crisis conundrum*. European Union Institute for Security Studies, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_2_Energy%20Crisis.pdf, retrieved on 12 May 2024.
45. Rid, T., Hecker, M. (2021). *The rise of hybrid warfare*. Oxford University Press.
46. Rouvinski, V. (2019). *Russian-Venezuelan relations at a crossroads*. Woodrow Wilson International Center for Scholars, Latin American Program, 1.

47. Rozental, D., Jeifets, L. (2022). *Russia and Venezuela: Russia's Gateway to Latin America*. In Rethinking Post-Cold War Russian – Latin American Relations (pp. 193-205). Routledge.
48. Schmidt, J.D. (2008). *China's soft power diplomacy in Southeast Asia*. The Copenhagen Journal of Asian Studies, 26(1), pp. 22-49.
49. Shan, A., Myeong, S. (2024). *Proactive threat hunting in critical infrastructure protection through hybrid machine learning algorithm application*. Sensors, 24(15):4888, p. 5, https://doi.org/10.3390/s24154888, retrieved on 12 May 2024.
50. Spataro, J.G. (2019). *Iranian Cyber Espionage*. Utica College ProQuest dissertations & theses, https://www.proquest.com/openview/7816e26f17ba341674713046f4a249fa/1?pq-origsite=gscholar&cbl=18750&diss=y, retrieved on 22 May 2024.
51. Starodubtseva, A. (2021). *Russian hybrid warfare in Ukraine: Comparative analysis of two cases and identification of critical elements in the successful application of hybrid tactics*. Master thesis, Praga: Charles University, Faculty of Social Sciences, Department of Security Studies, https://dspace.cuni.cz/bitstream/handle/20.500.11956/124589/120381167.pdf?sequence=1&isAllowed=y, retrieved on 22 May 2024.
52. Stokel-Walker, C. (2024). *Medical misinformation on social media – are the platforms equipped to be the judge?,* The BMJ, 2024, DOI: 10.2196/17187.
53. Suarez-Lledo, V., Alvarez-Galvez, J. (2021). *Prevalence of health misinformation on social media: systematic review*. J. Med Internet Res 2021; 23(1): e17187, https://www.jmir.org/2021/1/e17187, retrieved on 22 May 2024.
54. Thurston, A., Lebovich, A. (2013). *A handbook on Mali's 2012-2013 crisis*. Institute for the Study of Islamic Thought in Africa, https://sahelresearch.africa.ufl.edu/wp-content/uploads/sites/170/ISITA-13-001-Thurston-Lebovich.pdf, retrieved on 12 May 2024.
55. Tsiklauri, G. (2021). *Hybrid Warfare in Cyber domain: Case Study of hybrid threats in cyberspace.* Master thesis, Praga: Charles University, Faculty of Social Sciences, Department of Security Studies, pp. 42-48, https://dspace.cuni.cz/bitstream/handle/20.500.11956/127657/120387067.pdf?sequence=1&isAllowed=y, retrieved on 22 May 2024.
56. Vakarchuk, K.V. (April 2020). *The impact of the media on the Catalonia referendum*. Rhetoric and Communications, nr. 43, ISSN 1314-4464, https://rhetoric.bg/wp-content/uploads/2020/06/Vakarchuk-issue-April-2020-pp.83-95.pdf, retrieved on 12 May 2024.
57. Valenza, F., Karafili, E., Steiner, R.V., Lupu, E.C. (2022). *A hybrid threat model for smart systems*. In: IEEE transactions on dependable and secure computing, vol. 20, nr. 5, pp. 440 -4417, ISSN 1545-5971, Elettronico.
58. Vilmer, J.B.J., Conley, H.A. (2018). *Successfully countering Russian electoral interference*. Washington: Center for Strategic & International Studies, https://www.jbjv.com/IMG/pdf/180621_Vilmer_Countering_russiam_electoral_influence.pdf, retrieved on 12 May 2024.
59. Wentzell, T.D. (2021). *Russia's Green Men: The Strategic Storytellers of Hybrid Warfare*. Canadian Military Journal, 22(1), pp. 42-48, https://www.journal.forces.gc.ca/PDFs/CMJ221Ep42.pdf, retrieved on 22 May 2024.

60. Wither, J.K. (2016). *Making sense of hybrid warfare*. Connections: The Quarterly Journal, 15(2), pp. 73-87.
61. Wojnowski, M. (2021). *Russian interference in the U.S. Presidential elections in 2016 and 2020 as an attempt to implement a revolution-like information warfare scheme*, în US democracy as the target of Russian secret services, Warsaw Institute, Polonia, https://warsawinstitute.org/wp-content/uploads/2021/07/RS_06-2021_EN.pdf, retrieved on 22 May 2024.
62. Zdanowicz, M. (2023). *The migration crisis on the Polish-Belarusian border.* Białostockie Studia Prawnicze, 1(28), pp. 103-115, https://intapi.sciendo.com/pdf/10.15290/bsp.2023.28.01.06, retrieved on 22 May 2024.

USING TTX AS AN EDUCATIONAL TOOL IN THE FIELD OF INTEGRATED DEFENCE RESOURCE MANAGEMENT

Colonel Professor Dorel BADEA, PhD, BEng

Associate Professor Diana Elena RANF, PhD

Assistant Professor Elisabeta-Emilia HALMAGHI, PhD

Management Department, Military Management Faculty,
"Nicolae Bălcescu" Land Forces Academy, Sibiu

DOI: 10.55535/RMT.2024.4.36

The article deals with specific aspects of specialized military education, for the field of integrated management of defence resources. Particularities of a suitable educational tool in the field of security culture formation are presented through a flexible, less formalized character, from a procedural point of view. It is chosen as applicability, the field of defence resources, in a broad sense, emphasizing the need to pay more attention to the specific topics of preparing the national economy and the territory for defence. The research methods chosen as appropriate for this article are documentary analysis and case study. The main objective assumed by the group of authors is to support/reiterate the applicability of table top exercise in the field of military management.

Keywords: table top exercise; education; security culture; defence resources; management;

INTRODUCTION REGARDING THE TOPICALITY OF THE PROPOSED THEME

With the outbreak of the conflict in Ukraine, the specific problems of ensuring the resources of a complex war effort have returned to the present day, concrete examples in this regard being provided by the practice of military action by both belligerent parties. Complementarily, at the NATO level too, operational concepts related to military mobility, the transition to the war economy, resilience, public goods and public policies in the field of security, the relationship between the national economic capacity and military strategic framework, force generation and regeneration, new force management models etc. have been revitalised.

The management of resources for defence thus demonstrates its actuality, necessity and usefulness, the issue of interest stated before being largely subsumed, explicitly or implicitly, under this sector of activity. By the way, changing the discussion register at the national level, it is clearly stipulated in the defence planning documents, which also constitutes an argument for considering the management of defence resources in a much more comprehensive manner, the fact that: *"Integrated management of resources for defence is also achieved by maintaining an active link with the other structures in the national defence system, public order and national security or with responsibilities/tasks regarding national defence, both for the elaboration/application of operational plans and the use of forces, as well as for the establishment of non-military and production capabilities"*. (Ministry of National Defence, 2021, pp. 41-42).

It thus becomes imperative that the future officer (who is in the stage of training at the bachelor's level) has the minimum knowledge necessary to understand some fundamentals of the problem of resource management for defence, in peacetime as well as in wartime. Of course, it is necessary to have continuity in this sense at the level of the other career courses, correlated to their specifics. Subjects such as mobilization reserves, defence industry, institutional attributions in the management of different states of national security (crisis, emergency, war etc.), defence capabilities, requisitions are necessary to be part of the knowledge baggage of any officer, at different levels of detail, corresponding to the level

and type of training completed. The human resources management, a component of the integrated management of defence resources and one of the directions of action of this sector of activity, stipulated in the same programmatic document cited above, is defined as follows: *"The management of the military educational system will follow the change of the training paradigm, by directing the resources towards the training and professional development of leaders, warfighters and specialists capable of achieving success in a constantly changing operational environment, having the professional skills necessary to carry out missions now and in the future".* (Ib., p. 44).

The role of human resources in the integrated management of resources for defence must be seen in a broad framework, through the inter-conditions that occur both at the level of the processes and at the institutional level, of the organizational structures with attributions in different functional areas, institutions that finally compete to obtain a desired state. A useful approach in this sense is the systemic one *(figure 1)* in which we find both the practical component of the human resource activity in obtaining operational capability but also the one related to the skills needed by people in organizations, obtained starting from the training process.

We are talking in this framework of different generations in terms of expectations and perceptions regarding security, including motivation for the military career, for which a different educational paradigm is also needed in a complicated geopolitical context. How do we achieve the educational objectives assumed by the educational plans so that the graduate can cope with this reality as best as possible? How do we approach a balance between critical thinking and standard models or procedures for action? How do we reconcile the relationship between profession and occupation? These are legitimate questions, the solution of which leads to obtaining an educational profile adapted to contemporary reality, in which the security culture itself is in an increasingly accentuated dynamic. The means of cultivating the security culture are diversifying, both as a normal trend (the development of society itself) but also under the action of some influencing factors (also promoted by the development of IT technology means). There is a need for the future graduate to be exposed to diverse training contexts, situations and subjects in which, for their solution, they can use various means, tools etc. They include *table top exercise* (TTX will be used).

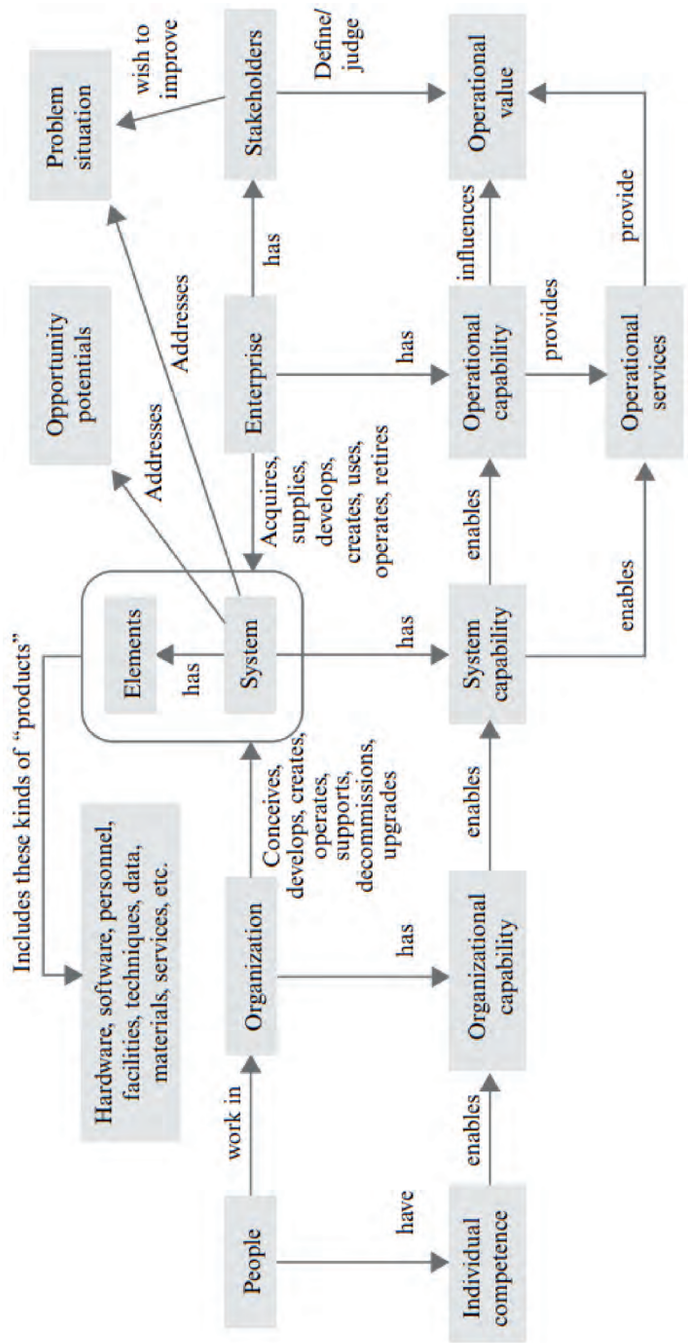


Figure 1: Conceptual model of systemic approach to human resource as activities and training
(INCOSE SHE, 2023, p. 242)

CONCEPTUAL AND PRACTICAL FOUNDATIONS OF TRAINING USING TTX

In national educational practice it can be appreciated that TTX is less used if we refer to and consider the USA as an example of good practice, where it is used for training, especially for the security of critical infrastructures (for example, Federal Emergency Management Agency/FEMA), both in the military and in the civilian environment. Remarkable approaches at the national level are recorded through the efforts of institutions such as the New Strategy Center, the Center for the Study of New Generation Warfare and the Euro-Atlantic Center for Resilience. The involvement of the latter in the organization and deployment of TTX for crisis management with urban public administrations as training target and its involvement in collaborations with both civilian and military academic environments is auspicious. Looking at the topicality of the educational method, it is noted that (Švábenský, 2024, p. 1): *"tabletop exercises are an innovative teaching method used in practice for training teams in incident response and evaluation of contingency plans. However, tabletop exercises are not yet widely established in university education"*.

As a scope, TTX has a wide area of applicability and *"is intended to generate discussion and can be used to enhance general awareness, validate plans and procedures, assess the types of systems needed to guide the prevention of, protection from, mitigation of, response to, and recovery from a defined incident as well as to facilitate conceptual understanding, identifying strengths and areas for improvement, and/or achieving changes in perceptions"* (Sukhodolia, 2018, p. 121). For educational purposes in particular, the properties regarding the facilitation of awareness of some aspects of interest of a situation from the security and defence plan, in our case, should be noted, as well as regarding the way of understanding and perception of some phenomena, processes etc. The research team coordinated by Amélie Frégeau (2020, p. 1) emphasizes for the medical field the informal character of this type of training: *"TTX is a facilitated group discussion that simulates an emergency situation in an informal, stress-free environment, sometimes using a board game format, and aims to strengthen readiness to manage a health emergency".*

Approached as a separate category of simulation, *"TTXs are a type of relatively low-fidelity simulation involving human participants, where participants are presented with a situation or world state in each turn of play, whereby they can deliberate and test various ideas of how to best deal with the situation with minimal effort or consequence (e.g., a TTX of how to respond to a wildfire is cheaper*

and safer than actually starting and putting out a wildfire for training purposes)" (Dorton et al, 2023, p. 3).

From a military perspective, similarities to wargaming and suitability to training objectives and training target characteristics are brought into focus: *"A Table-Top Exercise (TTX) is a type of wargame analysis, but with a softer name that is more widely accepted within civilian circles. It is an organizational framework that helps implement institution's capacity and capability building goals. The choice of the education and training framework depends on the training objective and trainees' characteristics"*. (NATO STRATCOM COE, 2022, p. 6).

In the dynamics of the actual development of TTX, the injections are very important, as a means to see the reactions of the participants and to evaluate the level of achievement of the objectives, based on the decisions made and the interventions produced. By injection we mean (European Commission, Joint Research Centre, Dirgančius et al., 2024, p. 9) *"a short event story used to bring an incident to the players' attention for whom it was created (and from whom a reaction is expected). In other words, it is an incident with relatively small and local consequences that demands reaction from a selected part of the participants".*

CASE STUDY ON THE USE OF TTX IN HIGHER MILITARY EDUCATION

The case study proposed for presentation is based on the military educational reality. More precisely, within the study course, *Preparing the national economy and the territory for defence*, included in the curriculum of the Land Forces Academy, the last seminar class is allocated to an integrative seminar that takes place during the 90-minute time allocated to the respective didactic activity, with each seminar group. For two of the student groups, it was decided to carry out a mini TTX, after having been told about the particularities of the TTX exercise, during the lecture, while presenting the educational ways of preparing the population for action in security risk situations. The students were divided into groups *(figure 2)* representing different institutions with a role in security and defence management, institutions which exist, at local level, in Sibiu.

The scenario they were exposed to is set out below.

On 08/05/2024, the residents of Sibiu were informed (at 15:31) by the Roalert system about the imminence (starting at 16:00) of a storm, with massive waterfalls and hail in some places, with the manifestation of stormy phenomena. In the city of Sibiu, the final of the Romanian football cup is being held at the municipal stadium, expected to end at 4:30 p.m. A group of foreign citizens are protesting in the Sub Arini Park area about the employer's non-compliance with the assumed contractual

clauses and the support of the totalitarian regime in power in the country of origin. A military equipment convoy is stationed near the Sibiu airport, waiting for an aircraft from Warsaw to land, in order to take over a company of Romanian soldiers who will move to Cincu starting at 5:00 p.m. As a result of the prolonged drought and the high temperatures recorded during this period, the vegetation is dry and the effectives of the ISU (the General Inspectorate for Emergency Situations), the county hospital and the Sibiu garrison, ensure water supply and medical assistance in the main areas of the city and in the neighbouring areas of Șelimbăr, Șura *Mică, Poplaca. The water levels of the Gura Râului dam are at the lower limit, as deficiencies (interruptions) in the supply of water to the water operator have been announced. The county prefect called the meeting of the committee for emergency situations at 4:00 p.m.*

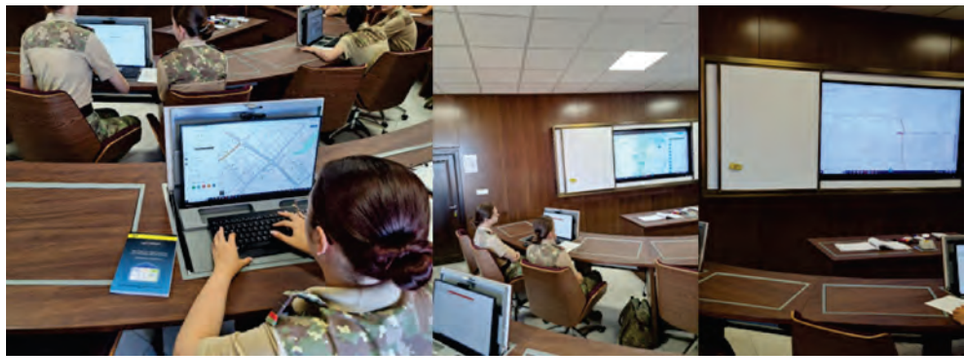


Figure 2: Images from the mini TTX exercise

The list of incidents that were played included:

1. *At 4:05 p.m., possibly due to the failure of some electrical transformers, an interruption of the electricity supply is observed in the area of the streets Revoluției, Dumbrăvii, Mihai Viteazu.*

2. *At the end of the football match, altercations started between a group of supporters and a group of demonstrators in the area of Hotel Sport. A gas pipeline in the area is heavily damaged.*

3. *The movement of the military convoy (approximately 12 technical vehicles accompanied by a military-police vehicle) from the airport begins (17.15). Groups of supporters blocked the roundabout near Ibis hotel.*

4. *The mayor of the commune of Poplaca, considering the damage caused by the storm, requests (19.00) the supply of essential products.*

As a procedure, after each incident, the working groups had 10 minutes to assess the situation and 10 minutes (all groups) to intervene and present a decision regarding the created situation. During the 10 minutes of analysis, they discussed and a member of the team prepared and shared on a PowerPoint presentation, the main ideas for discussion identified. As can be seen in *figure 2*, to identify the possible implications that different actions would have (and implicitly with the need for decision-making reaction), the cadet groups playing the role of security, defence, public order and national security institutions had the possibility of analysis using software like *Google Maps*, which also facilitates the creation of an overview of the area in question. In the preparation of the activities, prior to the TTX, the students were told that the area played would be the city of Sibiu and neighbouring areas. They were also asked, after establishing the group responsibilities (the institutions played), to document themselves regarding the powers and mode of action in the respective institutions.

The main observations noted by the coordinating teacher and students following the exercise were:

- the cadets' feedback was positive, being the first time (the first iteration) when they were exposed to such a training method, a fact ascertained during the deployment through their involvement and cooperation between teams and within the team;
- a classic hall (with a horizontal layout) is needed, the hall in which it took place being a mini-amphitheatre (with a semi-circular, tiered arrangement of tables), which obstructed group discussions and interaction with the other teams;
- certain operational sequences within the exercise exceed the level of knowledge possessed by the cadets, which can be remedied by more appropriate elaboration of the scenario and incidents or combining the teams, with officers participating in career courses organized in the same institution;
- a larger amount of time is required for deployment;
- for a more adequate immersion in the scenario, more audio-video means can be involved (e.g., reports, news etc.);
- being played with two groups, separately, it was possible to make comparative assessments regarding the interventions, team spirit, relevance of the proposed solutions etc.;
- there is also the option of conducting a TTX in parallel with other types of training exercises, with divided training objectives, conceptually subsumed

under a framework objective (it can be connected with training through virtual or constructive simulation);

- such a format can be replicated, adapted to the level of intellectual maturity of the students, both for groups of master's students from military academies and within the summer schools of military academies, or even in a military-civilian format with representatives of local public and private institutions, clearly correlated with the assumed training objectives;
- useful for training in a multinational framework is the POSEIDON/ Platform-based Operational System Events and Injects Distribution Online platform *(figure 3)* developed at the EU/Joint Research Center level for the management of training exercises, suitable for Erasmus type partnerships with military or civilian universities from Europe.

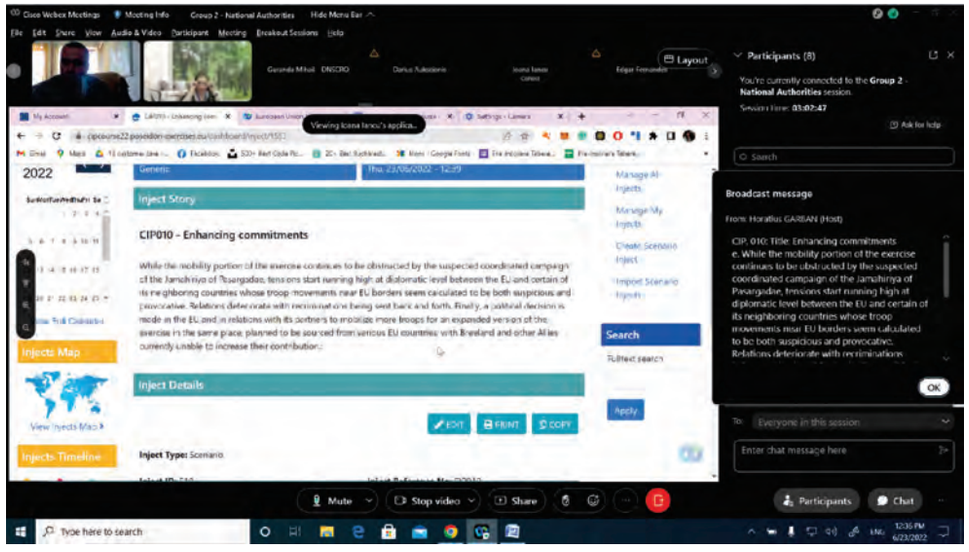


Figure 3: Use of the POSEIDON platform for TTX in the field of critical infrastructure protection
(generated during participation in an exercise)

CONCLUSIONS

The proposed educational tool is applicable in the field of integrated management of resources for defence, in the sense and context of those exposed, with differentiations, depending on the training target. Compared to other, much more formalized formats, it stimulates critical thinking. It is also suitable to use in the educational field to encourage teamwork, interaction and harmonization of ideas, especially useful for complex fields such as defence resources. Regardless

of how it is regulated at the international level (national guard, territorial forces etc.), the effort to augment the forces, means and processes specific to security and defence as well as the role of these types of structures in the management of crisis situations is increasingly important. In this sense, considering the decision-making specifics (the need for collaborative action) and the resources involved, it appears useful to replicate such situations, at levels appropriate to the training objectives, in the educational processes specific to military education, the tool presented having a flexible margin of applicability.

BIBLIOGRAPHY:

1. Dorton, S.L., Barrett, E., Fersch, T., Langone, A.&Neville, K.J. (2023). *RAD-XP: Tabletop Exercises for Eliciting Resilience Requirements for Sociotechnical Systems.* Systems, 11, 487. https://doi.org/10.3390/systems11100487, retrieved on 22 July 2024.
2. European Commission/Joint Research Centre, Dirginčius, E. et al. (2024). *Tabletop exercise: Coherent Resilience Baltic 2023 (CORE 23-B)*. Luxembourg: Publications Office of the European Union, https://data.europa.eu/doi/10.2760/702667, JRC137990, retrieved on 22 July 2024.
3. Frégeau, A., Cournoyer, A., Maheu-Cadotte, M. et al. (2020). *Use of tabletop exercises for healthcare education: a scoping review protocol*. BMJ Open. https://doi.org/10.1136/bmjopen-2019-032662, retrieved on 2 June 2024.
4. INCOSE SEH/Walden, D.D., Shortell, T.M., Roedler, GJ., Delicado, B. A., Mornas, O., Yip, Y.S.&Endler, D. (Eds.) (2023). *Systems Engineering Handbook: A Guide for System Life Cycle Process and Activities* (5th ed.). San Diego, CA: International Council on Systems Engineering. Published by John Wiley & Sons, Inc.
5. Ministerul Apărării Naționale/M.Ap.N./Ministry of National Defence (2021). *Carta albă a apărării/Defence White Paper*. București: Monitorul Oficial, Partea I no. 499 on 13 May 2021**.**
6. NATO Strategic Communications Centre of Excellence/NATO STRATCOM COE. (2022). *Constructing a table top exercise* (TTX), Riga.
7. Sukhodolia, O. (2018). *Training as a Tool of Fostering CIP Concept Implementation: Results of a Table Top Exercise on Critical Energy Infrastructure Resilience*. Information & Security: An International Journal, 40(2), pp. 120-128, https://doi.org/10.11610/isij.4009, retrieved on 22 July 2024.
8. Švábenský, V. et al. (2024). *From Paper to Platform: Evolution of a Novel Learning Environment for Tabletop Exercises*. Proceedings of the 2024 on Innovation and Technology in Computer Science Education, pp. 213-219. Online publication date: 3-Jul-2024. https://doi.org/10.1145/3649217.3653639, retrieved on 22 July 2024.

THE STRATEGIC RELEVANCE OF NATIONAL DEFENCE INDUSTRY IN MAJOR DEFENCE PLANNING DOCUMENTS – A CONTEXTUAL APPROACH –

Associate Professor Gabriel MĂNESCU, PhD
Military Management Faculty, Management Department,
"Nicolae Bălcescu" Land Forces Academy, Sibiu
Colonel Associate Professor Dumitru IANCU, PhD
Military Management Faculty, Management Department,
"Nicolae Bălcescu" Land Forces Academy, Sibiu
DOI: 10.55535/RMT.2024.4.37

In a world characterized by dynamism and increasing security challenges, the role of the national defence industry is becoming progressively vital in ensuring a nation's military capabilities. The present paper aims to analyse the current and future elements of the national defence industry, in terms of achieving, maintaining and developing our country's military capabilities against the backdrop of a volatile security environment. We also intend to analyse the relevance of the defence industry through the lens of the connections between this sector of activity and the main defence planning documents in force at this date as well as the strategic projects currently under public debate.

Keywords: defence planning documents; defence industry; strategy; strategic projects; security environment;

INTRODUCTION

The national defence industry plays an essential role in ensuring the security and sovereignty of a country, and its relevance has increased significantly in the current geopolitical context, characterized by international tensions and regional conflicts. In a constantly changing world, where cyber threats, terrorism, and armed conflicts are at the fore, states are forced to re-evaluate their defence capabilities and develop new, effective strategies, better tailored to respond to these challenges.

In this context, defence planning documents become crucial tools for the integration and coordination of available resources, including those of the national defence industry. These documents must reflect not only the immediate needs of national defence and security, but also the long-term vision of developing an industry capable of innovating and rapidly adapting to new technologies and strategic requirements.

In Romania, the relationship between the defence industry and planning documents is essential to ensure a balance between national independence and international cooperation, especially in the context of NATO and EU commitments. Therefore, a contextualized approach to this relationship can provide a better understanding of the current challenges and opportunities for developing an efficient and sustainable defence industry.

THE NATIONAL DEFENCE INDUSTRY – HISTORICAL LANDMARKS

Historically, we believe that the national defence industry has undergone several stages. From this perspective, we highlight the **year 1918**, the year of national reunification, as relevant for our study, even if various sources indicate the presence on the territory of the Romanian Principalities of weapons production workshops since the 18th century. Such an example is the Cugir Mechanical Factory whose history stretches since 1799 during the Austro-Hungarian Empire, in the form of steel production workshops built in Cugir, which were among the first metallurgical factories in Transylvania (UM Cugir, 2024).

Consequently, the evolution of the national defence industry could be grouped according to five main periods *(figure 1)*.

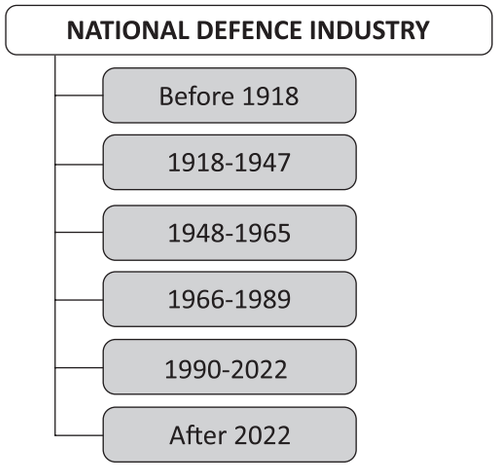


Figure 1: Stages in the development of the national defence industry
(authors' design)

Because the purpose of our approach is not to present in detail the evolution of the national defence industry, we will only briefly review the defining elements of each of the previously presented stages.

The period before 1918:

- after the Unification of the Principalities, in Muntenia and Moldova there were only rudimentary workshops that produced the gunpowder needed by the army. These inadequate facilities could not effectively supply the ammunition needed by a modern army;
- starting on 1/13 February 1861, in Bucharest, in the buildings of the former Mihai Vodă monastery, the first military workshops were inaugurated and tasked with carrying out repairs and producing equipment and harnesses for the army. Small workshops for the manufacture of ammunition and artillery materials also started to operate, and they will later form the basis for the Army Arsenal. These developments marked the beginning of the Romanian armaments industry;
- until 1865, the production of *bullets* was automated and carried out in Romania, which represented a significant step in the development of the national defence industry, ensuring the country's ability to independently produce essential military equipment for the army (Vințu, 2022);
- the first revolver of Romanian design was produced, under the guidance of artillery captain Vasile Buescu, known as *the BUESCU Revolver, model 1876, calibre 10.8 mm*;

- one of the most significant contributions of the Romanian specialists was the 75 mm calibre cannon, called the 1904 model. It represented an improved version of the *"Krupp"* cannon from 1889 and was considered the most advanced of that period, having a maximum range of up to 8,000 meters;
- however, when Romania entered the First World War, the Romanian Armed Forces were poorly trained, and their technical and armament equipment was not only insufficient, but often outdated both physically and morally.

The period between 1918 – 1947:

The achievement of the Great Unification at the end of 1918 was a crucial moment for the Romanian nation. After a war that they did not want, but that they had to fight in order to fulfil the dream of national unity, the Romanians finally saw their wishes fulfilled. The continuous efforts and sacrifices of hundreds of thousands of Romanians who fell on the battlefield were rewarded on 1 December 1918, when the process of Romanian national unification ended.

To strengthen the Romanian state after the Great Unification, King Ferdinand I and Romanian political leaders implemented a series of measures aimed at developing the national defence industry. It was essential to prevent the armaments and ammunition supply problems that the Romanian armed forces faced during the First World War.

In this regard, the Cugir-Copșa Mică Metallurgical Plants were established for the manufacture of armaments and infantry ammunition, under Czechoslovak license. In parallel, special production capacities were developed in Reșita and Bucharest. At I.A.R. Brașov began license production of Italian *"Savoia-Marchetti 79 B"* bombers and Polish PZL-11 fighters. At the end of the decade, serial production of the IAR-38 and IAR-39 observation and reconnaissance aircraft began, as well as of the IAR-80 fighter.

However, the production capabilities of the Romanian defence industry proved insufficient in the summer of 1940, when Romania faced threats to its national integrity. During those critical moments, the Romanian armed forces were still dependent on armaments, combat equipment, and ammunition from France, Great Britain, and former Czechoslovakia, which contributed to the acceptance of withdrawal without a fight from the territories claimed by the USSR, Hungary, and Bulgaria.

On 22 June 1941, when Romania entered the war alongside Germany against the USSR for the liberation of the Romanian territories across the Prut, the supply of armaments, combat equipment, and ammunition was insufficient to meet the requirements of the Romanian armed forces.

Between 1941 and 1944, the authorities in Bucharest worked to improve the production of their own armament and ammunition factories and to increase the quality of the manufactured products. During that period, the production of Romanian-designed combat equipment, such as the IAR-81 aircraft and the 75 mm *"Reșita"* anti-tank gun, also developed. Moreover, at the I.A.R. plant Brașov the German fighter plane *"Messerschmitt-109 G"* was assembled under license (Opriș, 2007, p. 6).

The period between 1948 – 1965:

It was one of the darkest periods in the entire history of the country. Thus, under the pressure of the Soviet political-military decision-makers, immediate after the end of the Second World War, the communist government led by Dr. Petru Groza decided to close most of the armament and ammunition factories in the country. Only the factory in Sadu (Gorj county), which produced infantry weapons and cartridges, and the *"30 Decembrie"* factory, specialized in the manufacture of cartridges, were kept in operation. The tools and installations from the closed factories that escaped being moved to Soviet Russia as payment for war reparations were dismantled, taken out of their sockets and stored in different locations. Meanwhile, the engineers and workers from those factories had to find other jobs, and spread out throughout the country (Ib., p. 8).

Aware of the importance of the special products needed by the Armed Forces and against the background of the introduction of *the five-year plans*, as engines of economic and social development, the leaders of those times ordered the reopening of certain enterprises, among which we mention: the factories *"6 Martie"* (Tohan, Braşov county), *"Ilie Pintilie"* (Plopeni, Prahova county), *"Bella Breiner"* no. 2 (Braşov), Târgovişte Metallurgical Plant, I.M.S. Sadu (Gorj county), I.M.S. Sadu (Pantelimon) and Cugir Metallurgical Plants (Sibiu county) (Ib., p. 10).

All the mentioned actions and measures had a huge cost for those times: about 92,000 kg of fine gold. Unfortunately, the five-year objectives were not achieved, so with the next plan, the objectives were resized to a three-year period (Ib.).

Another special element of those times was the decision of the Soviet leader, Joseph Stalin, who ordered the considerable increase in the military forces of Romania, Poland, Czechoslovakia, Hungary, and Bulgaria, as well as their equipment with Soviet weapons and combat assets, which generated increased imports of Soviet armaments and combat equipment. It led to huge increases in production costs, investments in various types of machinery that ultimately did not lead to the expected results, which translated into losses equivalent to approximately 17,000 kg of fine gold (Ib.).

The period between 1966 – 1989:

With the signing of the Warsaw Pact in 1955, Romania was assigned a series of tasks in terms of providing different categories of weaponry, equipment, and ammunition not only for the national armed forces but also for the armed forces of the other member states of the pact.

Obviously, in the beginning, armaments and equipment imports from the USSR were the most prevalent, but step by step, a large part started to be integrated into the national defence industry as a result of obtaining manufacturing licenses for them. In the beginning, a large part of the manufactured products was exported to the armed forces of some member states of the Warsaw Treaty Organization (Poland, D.R. Germany, Hungary, Czechoslovakia, Bulgaria). Aware of the lower quality of domestic products as compared to the Western ones, the party and state leadership made the decision to purchase equipment, machinery, and many aggregates from the West to be integrated into the Romanian industry. In fact, as a result of those measures, the conditions were created for *"Romania to pass from a five-year trade deficit of 118.8 million rubles (in its relations with the socialist states) to a surplus of 73.7 million rubles, at the end of the period 1966-1970"* (Ib., p. 33).

During that period, a series of essential special products for equipping the Romanian armed forces were designed and manufactured: the TR-580, TR-800 and P-125 tanks (variants of the T-55 and T-72 tanks respectively), the IAR-316 helicopters B *"Alouette III"* and IAR-330 H *"Puma"*, fighter-bomber aircraft IAR-93 B 111, amphibious armoured personnel carriers TAB-71 (BTR-60 APC)112, TAB-72, TAB-73 (with bomb launcher cal. 82 mm), TAB-77 and TAB-C (BTR-70), infantry fighting vehicle MLI-84 (BMP-1), many types of infantry weapons of different calibres, various types of chemical, bacteriological and radiological decontamination vehicles, mobile transmission stations, artillery technique and of course warships for the sea and river military fleet etc.

We believe that the mentioned period was the most prosperous stage in the existence of the national defence industry whose main coordinates can be summarized as follows:

- *"the Romanian armed forces were fully equipped with products and equipment manufactured by own defence industry at the level of the requirements of the Warsaw Pact;*
- *Romania ranked fifth in the top of the world's arms exporting countries, with the annual volume of exports exceeding USD 800 million;*
- *the results of military research found applicability in civilian production;*

- *part of the enterprises owned the production profiled on two branches, and thus the military capabilities were supplemented by the civilian ones;*
- *more than 200,000 employees worked in the defence industry;*
- *the personnel and production capacities were 100% met"* (Diaconu, 2016, p. 50).

The period between 1990 – 2022:

The revolutions of 1989 marked the end of Soviet rule and of the communist regimes in Central and Eastern Europe, paving the way for multi-party democracies and political systems based on free elections and civil rights. Those transformations contributed to the move from central to market economies, improving living standards and shifting the balance of global power in favour of liberal democracies, with a significant impact on society in areas such as education, media, and social structures.

The fall of the communist regime in Romania generated an extensive process of democratization and economic restructuring, which inevitably included the reformation or reduction of the defence industry. We believe that the main influences on the defence industry were:

❖ **The decline of the collaboration with the Soviet Union**: The close military collaboration with the Soviet Union, which provided equipment, know-how and resources, ended. It weakened the production capacity of the defence industry, making it more dependent on Western technologies and standards.

❖ **The reduction of defence spending**: In the context of the transition to market economies and the prioritization of spending for social and economic development, defence budgets were considerably reduced. It led to the decline of military production and consequently the closure of most factories in the defence industry.

❖ **The conversion of the defence industry**: Many factories that produced military equipment were forced to adapt and switch to civilian production, due to the decreasing demand for military equipment, as well as due to the new trade relations established with the West.

❖ **Integration into NATO**: In 2004, like most countries in Central and Eastern Europe, Romania joined NATO, which required the modernization of the armed forces and equipment, according to Western standards. It led to investments in the modernization of some segments of the defence industry, and especially to cooperation with the major international producers of armaments and military equipment.

❖ **The loss of traditional partners**: After the fall of the communist regime, those relationships ended or diminished considerably, directly affecting the production and exports of military equipment. The main effects were:

- *The end of the relations with the Soviet bloc*: The Warsaw Pact countries and the Soviet Union were Romania's main commercial partners in the defence industry. After the collapse of communism and the dissolution of the Soviet Union, Romania lost access to those traditional markets and, implicitly, an important source of revenue from military exports;
- *Declining demand for Soviet-style equipment*: Most of the equipment produced by Romania before 1989 was adapted or inspired by Soviet models. With the severing of ties with those markets and the adoption of Western standards, the demand for such equipment fell dramatically.
- *Change in strategic orientation*: After 1989, Romania began to re-orient towards NATO and the European Union, which required a change in the strategy of the defence industry. Instead of producing equipment for the traditional markets in the former Soviet bloc, the Romanian industry had to adapt to Western requirements and standards. The process was slow and difficult, mainly due to the lack of investments and modern technologies, but above all, because a medium and long-term vision did not exist.
- *Factory closures and reduced production*: With no steady demand and access to traditional markets, many factories in the defence industry were closed or significantly reduced their activity. It led to a massive restructuring of the sector, and consequently, many workers and specialists were affected.

In what concerns the latter aspect regarding the massive restructuring of the workforce in the defence industry, we can argue that the situation is almost identical to that of the late 1940s, *"so that by the year 2000 more than 52,000 employees were laid off, not keeping account of the personnel structure, primarily targeting directly productive personnel"* (Ib.).

In fact, *"in the past 30 years the number of employees has decreased from over 220,000 employees in 1989 to approximately 11,000 employees in 2022, the maximum average number of employees in the defence industry naturally followed a downward trend, registering a slight increase in 2022 when the maximum average number of employees reached 1,380 employees (figure 2), the financing being made from the budget of the Ministry of Economy in the amount of 77,400 thousand RON"* (Mănescu, 2023).

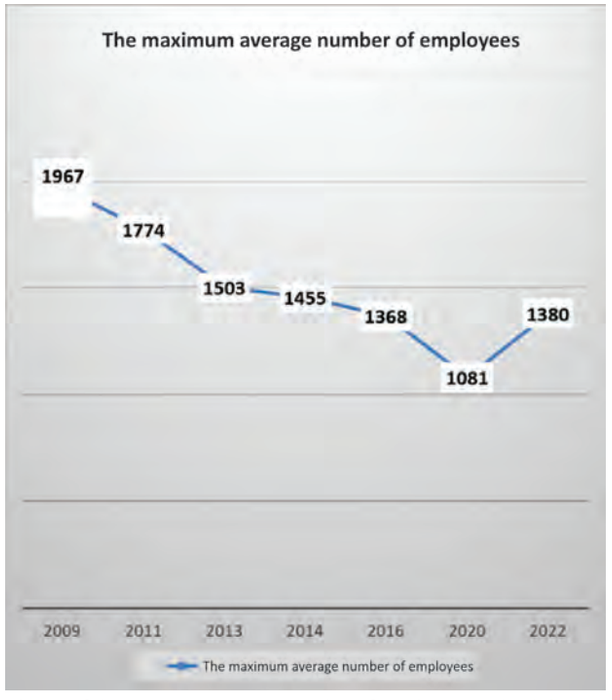


Figure 2: Evolution of the maximum average number of employees in the defence industry (lb.)

NATIONAL DEFENCE INDUSTRY AFTER 2022

We want to highlight this period separately because the start of the war in Ukraine had a significant impact on the entire Romanian society and, implicitly, on the Romanian defence industry, influencing both the demand for products and the level of activity of the companies involved. From our point of view, referring strictly to the defence industry, we believe that the main ways in which this conflict has affected this sector are represented by:

1. Increased demand for military equipment – The war caused an increased demand for military equipment throughout Europe, including Romania. NATO countries and other partners in the region have stepped up their rearmament efforts, and Romania's defence industry has received a boost, being asked to provide ammunition, military vehicles, protective equipment, and other products needed in the context of a high-intensity conflict.

As a NATO member state and a neighbour of Ukraine, Romania has played a particularly important role in providing logistical and military support to Ukraine, either through donations or direct sales of equipment. Thus, some companies

in the defence industry received additional orders both from the Romanian government and from NATO partners to supplement military stocks. However, the demand for armaments, ammunition, and various categories of military equipment is so great that no European or NATO state can meet the demand without significantly reducing its own stocks – with direct consequences for national security, and without involving huge expenses for their production or acquisition, individually or jointly, as is the case with the European Union plan launched at the end of March 2023, when EU defence ministers approved a plan to send Ukraine one million 155 mm artillery shells in the next 12 months. Unfortunately, problems related to production and logistics capacities meant that this target was only 52% accomplished, which means approximately 524,000 shells (Mureșan, 2024).

2. International partnerships and foreign investment – The war has emphasized the importance of collaboration between defence companies from different NATO states. Romania has become an attractive destination for investments and partnerships with foreign defence companies. Romanian producers benefited from technology transfers, partnerships with companies from the USA, France, Germany and other NATO countries, which helped to modernize production processes and increase competitiveness.

For example, on 22 May 2024, the Government of Romania *"signed two memoranda of understanding between the Romanian defence industry and foreign manufacturers. One is between the Cugir Mechanical Plant and Hekler & Koch GmbH (Germany). The second is Romaero and Aeroplex of Central Europe Aircraft Technology Center (Hungary)"* (Tudorică, 2024).

3. Revival and modernization of the defence industry – In the context of increased geopolitical tensions, Romania has begun to pay more attention to the modernization of its own defence capabilities. In recent years, there has been an increased concern about increasing the defence budget, and the war in Ukraine has accelerated this process. The Romanian government announced its intention to increase defence spending to 2.5% of GDP, which brought opportunities for local industry.

Thus, thanks to the partnerships concluded with external partners, state factories such as Uzina Mecanică Plopeni, Aerostar and Romarm began to play a more important role, contributing to modernization projects of Romanian military equipment and supplying components and equipment for the allies.

4. Increasing production capacities and the renewing of the infrastructure – Many Romanian armaments and military equipment factories, which in the past faced financial and technical difficulties, received a new boost due to the increased

demand for these types of products. Some of them have invested in the modernization of production lines so as to be able to face internal and external requirements or benefit from the investments made by foreign partners.

Eloquent in this sense is the transaction by which the German arms and military vehicle manufacturer Rheinmetall acquired this year the majority stake of the Romanian vehicle manufacturer Automecanica Mediaș, the new company going to be named Rheinmetall Automecanica. *"Through this transaction, the factory in Mediaș will have a key role in maintaining the operational readiness of the combat vehicles built in the West for Ukraine, as well as in ensuring logistical support, and the forces deployed on NATO's eastern flank will be able to count on faster response times and on more robust supply chains. In addition, Rheinmetall will now be a main partner of the Romanian armed forces as well as of neighbouring countries, with a significantly expanded range of products and services"* (Dincă, 2024).

We must also state that the Rheinmetall Lynx armoured combat vehicle, the HX 2 truck and the RAM container trailer will be produced in Mediaș. Although these products are not part of the Romanian armed forces (at least not for now), the development of these programs in our country represents a huge step for the national defence industry.

Furthermore, in the direction of increasing production capacities and renewing the infrastructure, we must highlight a particularly gratifying fact, namely the resumption of production of explosive powders. The investment of over 400 million Euros would also be made by the Germans from Rheinmetall, in Victoria, on the site of the former Pirochim powder factory, thus resuming an old tradition interrupted more than 20 years ago (Spotmedia.ro, 2024).

5. Political and strategic relations – In addition to the economic factors, the war has also amplified Romania's political and strategic cooperation with NATO allies and the European Union. Romania became an important logistic hub for the transport of military aid to Ukraine, and it also involved collaborations with the industrial sector for the transport and delivery of equipment, the development of road, rail, and naval transport infrastructure.

CONNECTIONS BETWEEN DEFENCE PLANNING DOCUMENTS AND THE NATIONAL DEFENCE INDUSTRY

It is well known that the national defence industry represents a *"strategic domain of the national economy that includes economic operators, regardless of the structure of the social capital, which have the technological, organizational, and management resources necessary to create and supply to the FSNA* (force structures

in the national defence system) *with military, sensitive and strategic products, as well as the necessary services"* (Parliament of Romania, 2016). Throughout its existence, it has gone through several stages whose general characteristic was or is similar to that of Romanian society at that time.

From the perspective of the strategic approach of the national defence industry, we aim to illustrate the relevance of this field in defence planning documents in the following section.

As mentioned in art. 3, paragraph (1). Of *Law no. 203 of 16 July 2015, regarding defence planning, "documents for defence planning at the national and departmental level take into account the obligations, requirements, and recommendations"* of documents of strategic importance developed at NATO and European Union level or as a result of agreements/partnerships concluded with different states, or responsibilities resulting from membership in different international organizations. The content of such documents is classified, for obvious reasons; however, some of these documents and especially those developed by the European Defence Agency (EDA) are public and (based on the principle of decision-making transparency) offer the general public information about the measures and activities undertaken in its area of responsibility.

Thus, one of the most important EU projects carried out through the EDA is the one related to the ***First Defence Industrial Strategy and a New Program for the Defence Industry to Increase the Degree of Readiness and Security of Europe***. The document *"sets out a clear, long-term vision to achieve defence industrial readiness in the European Union"* (European Commission, 2024-a) whose directions for the next ten years are based on four pillars: *increased investment, quality (better), collaborative (together) and European.* Naturally, the strategy also presents *"main directions to follow and the set of indicators by which the progress made by the member states in the direction of industrial preparation can be measured"* (Ib.).

The European Defence Industry Program (EDIP) is a new legislative initiative designed to ensure the transition from short-term emergency measures, adopted in 2023 and valid until 2025, to a structural and long-term approach, aiming to achieve an adequate level of industrial training in the defence sector. It will guarantee continuity of support for the European defence industrial and technological infrastructure, facilitating its rapid adaptation to the new realities (European Commission, 2024-b).

The main financial aspects of the EDIP aim at:

- mobilizing 1.5 billion EUR from the EU budget between 2025 and 2027;

- improving the competitiveness of the defence industrial and technological infrastructure in Europe (European Defence Technology and Industrial Dependencies, EDTIB);
- expanding the logic of the interventions implemented by the European Defence Industry Reinforcement through common Procurement Act (EDIRPA) (financial support to simplify the cooperation of member states in the public procurement phase);
- Act in Support of Ammunition Production (ASAP) (financial support for defence industries that increase their production capacity);
- supporting the industrialization of products resulting from cooperation in research and development, financed by the European Defence Fund (European Commission, 2024-b).

The EDIP budget can also be used to *"create a fund dedicated to accelerating the transformation of defence supply chains (FAST). This fund will facilitate access to loan or equity financing for SMEs and mid-cap companies developing defence technologies or manufacturing defence equipment. At the same time, EDIP will strengthen the EU's industrial cooperation with Ukraine in the field of defence and support the development of its defence industrial and technological base. To this end, the program could benefit from additional funding from the exceptional profits generated by immobilized Russian assets, depending on the decision of the Council, on the proposal of the High Representative"* (Ib.).

The Relevance of the Defence Industry in National Defence Planning Documents

The planning documents at national level are the *National Defence Strategy of the Country* and the *Government Program*.

The National Defence Strategy of the Country for the period 2020-2024 mentions the notion of industry eight times in its pages. One mention associates it with the concept of *security industry*, another one links it with *industrial cooperation in the field of defence* and defence-related fields, and one mention refers to the fact that *"the existence of important resources intended to equip the Romanian Armed Forces and the guarantee of their long-term provision represent an impetus necessary for the revival of the national defence industry"* (Presidential Administration, 2020).

In regard to the second programmatic document at national level, the *Government Program,* the document developed by the current governing coalition, chapter 5, relating to the Ministry of Economy, Entrepreneurship and Tourism, mentions that *"the national defence industry can produce and work to cover the needs of the MoD, in close collaboration with it, and also those of the external*

markets. Only vision and good faith and honest interest are necessary" (Government of Romania, 2023, p. 37).

In the same document, chapter 17, reserved for the Ministry of National Defence, contains no explicit mention of any collaboration between the Ministry of Defence and the National Defence Industry. Nonetheless, it reiterates part of the strategic directions presented in the *National Defence Strategy of the Country for the period 2020-2024*, and enumerates a series of agreements between the Romanian government and various international bodies, future projects etc.

Given that the two documents are of a programmatic nature, expressing intentions, the second one having a declared duration of only one year, and considering that the application of the provisions of the latter depends on the situation of the governing party/coalition, we mention that they have the merit of not having omitted this area which is extremely important for the country.

The Relevance of Defence Industry in Departmental Defence Planning Documents

"The main documents that underpin defence planning at the departmental level are:

a) The White Paper on Defence;
b) The Military Strategy;
c) The Defence Planning Directive;
d) Major Programs;
e) Annual plans" (Romanian Parliament, 2013).

These documents developed at the MoD level have the role of transposing the vision and directions of action specified in the documents developed at national level into concrete measures and actions in the field of national defence.

The *White Paper on Defence* aims to establish an integrated and complete set of measures and actions for the medium and long term in the field of defence, with the objective that the Armed Forces of Romania are equipped in such a way that they are able to protect vital national interests whenever necessary. The document refers to the defence industry no less than 15 times during the chapters dedicated to the directions of action for the development of defence capabilities and the integrated management of defence resources. Most often, references are made to *"increasing the degree of involvement of the national defence industry in carrying out the equipment", "the involvement of economic operators from the defence industry in public-private partnerships on the CDI dimension", "the development of technologies at the level of the MoD"* and, in the words of the Minister of Defence at the time, *"one of the essential elements, the development of which is consistently*

*pursued in the present defence planning document is ... a strong domestic defence industry...." (*Ministry of National Defence, 2021-a)

On the other hand, *Romania's Military Strategy, 2021 edition*, takes ideas from the two previously presented documents, making 12 references to the defence industry. What has particularly attracted our attention is that the *"inconsistencies between the level of the national defence industry's capacity to produce weapon systems, combat equipment, equipment and materials, on the one hand, and the needs of the Romanian Armed Forces, on the other hand"* (Ministry of National Defence, 2021-b) are considered vulnerabilities with a direct military effect, which in our view is actually an official acknowledgment of the big, serious problems facing the national defence industry.

The other departmental documents tackle the concept of the defence industry to a lesser extent, as their role is to specify the *main major programs* and especially the *essential programs* that contribute to their fulfilment, going into detail in the *annual plans*, subsequent to each program.

What are the main take-aways from the analysis of these strategic documents regarding the defence industry?

First of all, the fact that its mention in defence planning documents at national and departmental level underlines the essential role of this sector of activity in ensuring and developing national military capabilities.

Secondly, it is reiterated that the modernization and technological development of the armed forces can only be achieved through close collaboration between the public and private sectors, and last but not least, the fact that the two previously stated objectives constitute the foundation of Romania's national security and strategic resilience.

Strategy for the Defence Industry 2024-2030

The document developed by the Ministry of Economy, Entrepreneurship and Tourism, posted on the institution's website for public consultation, appears at a time when the global security landscape is marked by deep uncertainties and emerging risks. The strategy should anticipate both present and future challenges, and be built on solid principles and conceptual clarity, which will contribute to the affirmation of Romania as a pillar of security and stability on the eastern border of the Euro-Atlantic community.

Although the introductory part of the Strategy respects the generally accepted and recognized norms for such a document, in reality, however, the document does not present any vision or ambition, being devoid of prospective capacity and anticipatory character – essential elements both for economic agents

and for international partners. These elements are necessary to encourage relevant and sustainable technological investments and collaborations for the medium and long term. From our point of view, the stated duration of the strategy – 6 years – is totally unrealistic considering the tortuous legislative path it must go through and the present economic-military dynamics which, from the very beginning, make the strategy's horizon insufficient to achieve significant changes in this field.

The emphasized strategic priorities aim at the *"resumption of powder manufacturing", "transformation and revitalization of infantry armament manufacturing capacities", "transformation and revitalization of ammunition production capacities", "transformation and revitalization of aeronautical production capacities"* (Romanian Government, 2024). The same *"transformation and revitalization"* syntagm is obsessively repeated, in each and every priority, as a reminiscence of the past which we cannot detach from (Iancu, 2024).

Essentially, this strategy reflects a chronic inability to adapt the Romanian defence industry to European dynamics. The problem is not only that the document almost completely ignores the EU's defence technological and industrial integration mechanisms, but also the increasingly unpredictable and turbulent security environment, with a war raging on our country's borders. Thus, in our opinion, the *National Strategy for the Defence Industry 2024-2030* isolates us even more from the communities of values and interests which Romania is a part of.

CONCLUSIONS

The decline of the defence industry in Romania that began in the '90s has influenced not only this sector of activity but also the economy in general, with dramatic social effects.

The causes are multiple. Starting from the loss of traditional partners during the Cold War, the restructuring of the armed forces and, implicitly, the significant reduction of military expenditures, they have all led to a decrease in domestic demand and to the neglect of the development of own military production capacity. On the other hand, Romania has relied excessively on the guaranteed support of NATO, underestimating the importance of maintaining an autonomous and functional defence industry.

The constant decapitalization of the defence industry and the lack of orders from the Ministry of National Defence have severely limited the production capacity and greatly reduced the modernization chances/opportunities. Focusing on expensive import purchases, without activating the offset clauses that could have contributed to the relaunch of the national defence industry, represented a missed opportunity

for the sector's long-term development. In addition, the lack of competence in the state structures responsible for the defence industry and the inefficient management of resources have contributed to the delay in the modernization process of this vital sector of national security. Badly managed or unduly delayed decisions have accentuated the vulnerability of an industry that should have played a key role in the context of today's security challenges.

The increase in demand for military equipment, fuelled by the outbreak of the war in Ukraine, highlighted the vulnerabilities of the Romanian industry, which could have played an essential role in strengthening national security, but was affected by the lack of coherent strategies and the insufficient involvement of political and military decision-makers. The inability to formulate and implement clear long-term plans has significantly reduced the industry's ability to respond quickly and effectively to new challenges and opportunities.

While hesitant and uncommitted political decisions blocked the processes needed to revitalize the defence sector, the private sector began to play an increasingly visible role in the contracts for the maintenance and modernization of military equipment. Companies such as Elmet International, Aerostar Bacău and ProOptica have demonstrated the ability of the private sector to take over part of the responsibilities that the state has not been able to manage effectively. These companies, and not only, seem to know better the real needs of the military in terms of equipment and technology. Moreover, they demonstrate not only that they have the ability to deliver quality products, but also their commitment and better understanding of reality and, above all, vision.

In the current context of regional and global security, Romania needs a strategy that generates trust, promotes international collaboration and is built on solid principles and conceptual clarity. A modern strategy, based on innovation and competitiveness, will become a pillar of security and stability on the eastern border of the Euro-Atlantic community, and a catalyst for significant funds available on the global arms market.

Such a strategy could propel the Romanian defence research and industry into leading positions in European consortia for the development of future strategic defence systems.

BIBLIOGRAPHY:

1. Presidential Administration (2020). *Strategia Națională de Apărare a Țării pentru perioada 2020-2024/National Defence Strategy for the period 2020-2024.* București, https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_Tarii_2020_2024.pdf, retrieved on 28 August 2024.

2. European Commission (2024-a). *Prima strategie industrială europeană în domeniul apărării la nivelul UE/The European Defence Industrial Strategy,* https://romania.representation.ec.europa.eu/news/prima-strategie-industriala-de-aparare-si-un-nou-program-pentru-industria-de-aparare-pentru-spori-2024-03-05_ro, retrieved on 28 August 2024.
3. European Commission (2024-b). *European Defence Industry Programme,* https://defence-industry-space.ec.europa.eu/document/download/638c4482-0715-4aef-ac86-6529ce2dfd4b_en?filename=DEFIS_EDIP_factsheet.pdf, retrieved on 28 August 2024.
4. Cugir, UM. (2024). *Despre noi*, https://umcugir.ro/despre-noi/, retrieved on 8 September 2024.
5. Diaconu, B. (2016). *Industria de apărare a României. Actualitate* și *orientări de persectivă.* In *Buletinul Universităţii Naţionale de Apărare "Carol I"*, pp. 49-55, retrieved on 15 May 2024.
6. Dincă, T. (2024). *Tranzacție finalizată – Rheinmetall cumpără Automecanica Mediaș. Compania românească își schimbă denumirea*, https://www.profit.ro/must-read/tranzactie-finalizata-rheinmetall-cumpara-automecanica-medias-compania-romaneasca-isi-schimba-denumirea-21666850, retrieved on 15 September 2024.
7. Government of Romania (2023). *Program de guvernare 2023-2024/Government Programme 2023-2024. Viziune pentru națiune. Partidul Social Democrat, Partidul Național Liberal,* https://gov.ro/fisiere/pagini_fisiere/23-06-16-12-32-52Programul_de_Guvernare_2023-2024.pdf, retrieved on 15 September 2024.
8. Government of Romania (2024). *Strategia națională pentru industria de apărare 2024-2030/National Defence Industry Strategy 2024-2930.* București, https://economie.gov.ro/21729-2/, retrieved on 15 September 2024.
9. Iancu, N. (2024). *Strategia națională pentru industria de apărare 2024-2030: O nouă strategie pentru trecut*, https://www.linkedin.com/pulse/strategia-na%C8%9Bional%C4%83-pentru-industria-de-ap%C4%83rare-2024-2030-nicu-iancu-ct8ue/, retrieved on 16 September 2024.
10. Mănescu, G. (2023). *Pregătirea economiei naționale și a teritoriului pentru apărare. Concepte fundamentale.* Sibiu: Editura Academiei Forțelor Terestre *"Nicolae Bălcescu".*
11. Ministry of National Defence. (2021-a). *Carta albă a apărării/White Paper on Defence.* București, https://www.mapn.ro/legislatie/documente/carta_alba_2021.pdf, retrieved on 15 September 2024.
12. Ministry of National Defence (2021-b). *Strategia militară a României/Romania's Military Strategy.* București, https://www.mapn.ro/legislatie/documente/STRATEGIA-MILITARA-A-ROMANIEI.pdf, retrieved on 16 September 2024.

ANALYSIS OF THE DEFENCE INDUSTRY OF THE RUSSIAN FEDERATION – IMPACT ON THE NATIONAL SECURITY OF ROMANIA –

Police Quaestor Cătălin ANDRUȘ, PhD
Director of the National College of Home Affairs, Bucharest, Romania
Police Principal Quaestor Ștefan SĂVULESCU, PhD
Lucian IVAN, PhD
National College of Home Affairs, Bucharest, Romania
DOI: 10.55535/RMT.2024.4.38

The Russian Federation allocates significant government funds for the development of the defence industry in order to successfully support the military conflict in Ukraine. In order to support the war effort, the Moscow authorities have ordered measures to strengthen the domestic defence industry, while at the same time purchasing certain military and dual-use products from strategic partners such as China, the Islamic Republic of Iran, North Korea, in order to cope with the sanctions imposed by the Euro-Atlantic states.

The Russian Federation's main strategic partner in Asia is China, which has given the necessary military aid to the Moscow authorities to support the military conflict in Ukraine, although the Beijing authorities are declaring that they support neutrality and a balanced approach to this war illegally waged by the Russian Federation in Ukraine.

The defence industry of the Russian Federation is capable of sustaining the military conflict in Ukraine in the long term, benefiting from research and development capabilities of military products and technologies, including on the basis of technological support received from China. In this context, it is necessary to take measures at the level of the Euro-Atlantic states to reduce the resilience of the Russian Federation's defence industry, including by adopting additional sanctions against the Russian Federation and its allies, which would have a direct impact in reducing the production of military equipment and munitions.

Keywords: defence industry; national security; analysis; Russian military complex; resilience;

INTRODUCTION

The military conflict launched by the Russian Federation in Ukraine on 24 February 2022 requires both sides to allocate substantial additional resources dedicated to the acquisition of high-performance military equipment and ammunition. In this context, in order to be able to anticipate the actions of the Russian Federation on the Ukrainian front, as well as the future actions of the Kremlin authorities, it is necessary to conduct a comprehensive analysis of the potential of the Russian defence industry and the resilience of this industrial branch. While Ukraine is highly dependent on modern weaponry and ammunition supplied by Western states, the Russian military complex is capable of providing the Russian armed forces with much of the military equipment and ammunition necessary for the continuation of the war over a long period of time.

In fact, the tactic of the Russian Federation in the war in Ukraine is to prolong the military conflict for a long period of time, relying on the fact that the population in the Western states supporting Ukraine with arms and ammunition will react negatively to the steps taken by their own governments, as well as on the constant support for the Russian military from Russia's strategic partners, mainly China, the Islamic Republic of Iran and North Korea.

The analysis of the Russian Federation's 2024 budget allocations for national defence reveals the interest of the Kremlin military authorities to continue the war in Ukraine by allocating 7.1% of GDP or about 21% of government spending to this strategic objective. At the same time, estimates for the period 2025-2026 reveal the allocation of substantial funds for the continuation of the military conflict, with military spending in 2025 estimated at 25% of total government spending (8,534 billion rubles) and 21% (7,409 billion rubles) in 2026.

On the other hand, NATO member states still do not allocate sufficient resources for defence, as there are ongoing negotiations at the alliance level for the allocation of at least 2% of GDP to defence by all member states. In this context, it is necessary to understand the real danger posed by the expansionist policy of the Russian Federation and to raise awareness among policy makers and the population of NATO member states of the importance of cooperation between companies

in Western countries for the rapid development of new military technologies that will deter Russia from attacking a NATO member state in the medium and long term. From this point of view, Romania has understood the importance of allocating additional resources for equipping the Romanian armed forces, with 2.5% of GDP being adopted, by legal regulations, for the defence sector. It is important for Romania that a consistent part of these budgetary allocations in the field of defence should be allocated to modernizing the armed forces, through the acquisition of modern military equipment that will deter Russian armed forces from attacking the national territory. Also, important resources have been allocated at the governmental level for the recovery of the Romanian defence industry, including through the drafting of a new strategy for this area of strategic interest. It is essential for Romania to rely on its own defence industry, which needs to be modernized by establishing profitable public-private partnerships by attracting powerful investors from the Euro-Atlantic area to our country. In this way, Romania will benefit from the transfer of the know-how needed to modernize its armament and ammunition production sections and to develop specialized facilities for the maintenance of imported equipment (e.g. the F-16 multirole aircraft, which Romania has acquired from the USA, and the preparation of facilities for the repair of the F-35 multirole aircraft that Romania is to acquire in the coming period).

Another important aspect that needs to be analysed is the level of response of the Russian Federation's strategic, but above all tactical, nuclear forces. Although the probability of a nuclear-weapon attack against Ukraine, and NATO and EU member states is low, it cannot be neglected, taking into account the regulations contained in the Russian Federation's defence strategy, which stipulates that a nuclear-weapon attack is possible in a situation where Russia's national security is endangered. The recent attacks by Ukrainian armed forces on the territory of the Russian Federation are regarded by the Moscow authorities as an attack on Russia's national security, which creates favourable conditions for a nuclear attack with tactical nuclear weapons. If the Russian Federation decides to launch a nuclear attack with tactical nuclear weapons, the main target will be the Ukrainian capital Kyiv. This hypothesis is based on the assumption that a nuclear attack must induce a particular impact that would tip the balance of war in favour of the Russian Federation.

ANALYSIS OF THE DEFENCE INDUSTRY OF THE RUSSIAN FEDERATION

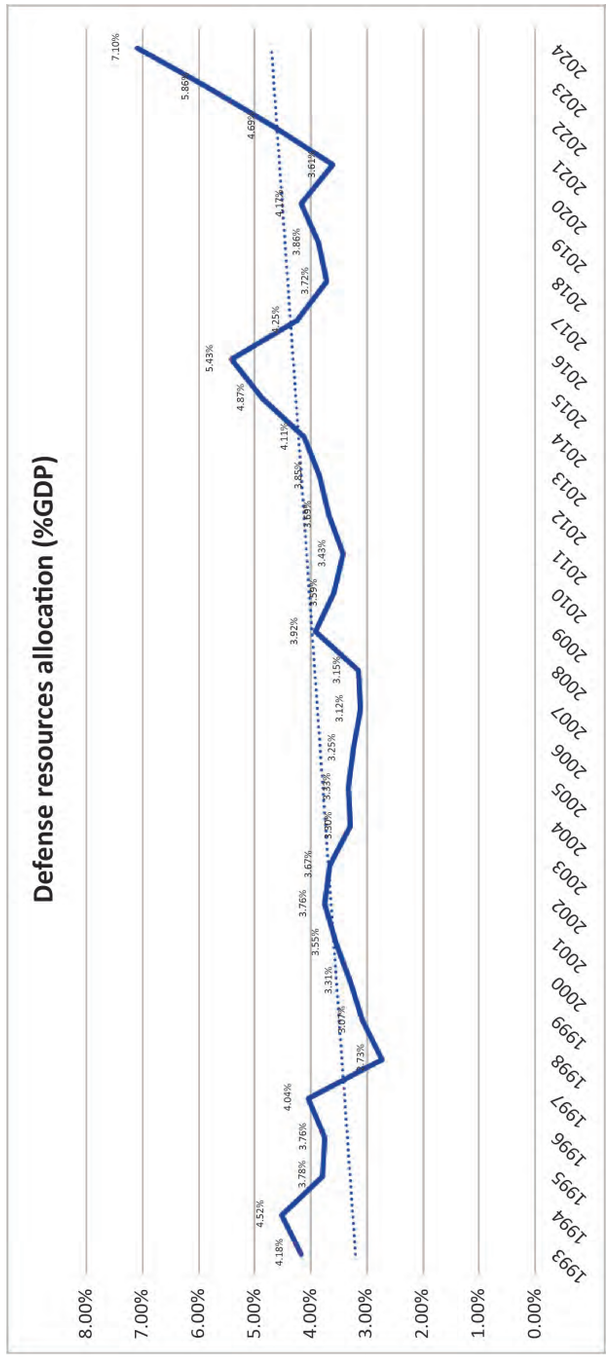
In order to make a comprehensive analysis of the Russian Federation's defence industry, a quantitative approach is necessary in order to correctly identify the risks to the EU, NATO and, implicitly, to Romania's national security.

The data used in this quantitative analysis are collected from the website of the Stockholm Institute for Peace Research Institute (SIPRI), a Swedish non-governmental organization specialized in the analysis of defence industry data, with over 50 years of experience in the field.

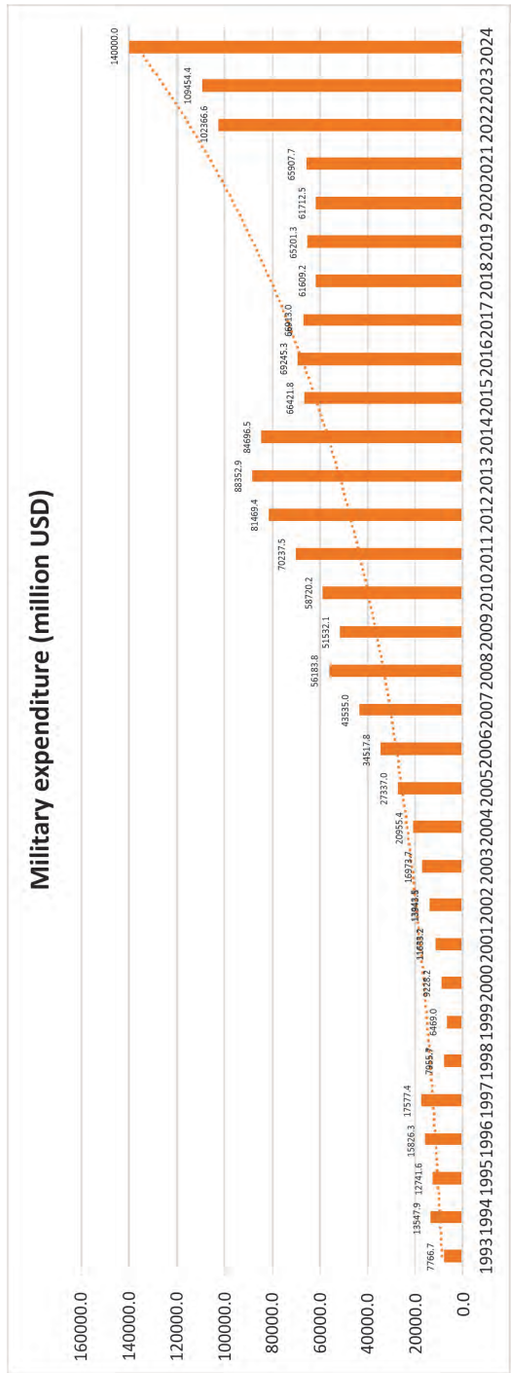
According to the data provided by SIPRI, the analysis of the last four years in terms of the percentage of GDP allocated to defence by the Russian Federation shows a sharp increase from 3.61% (2021) to 4.59% (2022), 5.86% (2023) and an estimated 7.1% in 2024. These data confirm the Russian Federation's interest in investing considerable sums in the defence sector, i.e. in the Russian military complex, which has recently shifted to war production, becoming a priority area for the Moscow authorities. In this context, the capacity of the Russian defence industry to produce large quantities of modern military equipment and ammunition needed to supply the military forces in Ukraine should by no means be underestimated.

There is a superficial tendency among some Western experts to underestimate the Russian military complex's ability to produce high-performance military equipment, despite the fact that the Russian defence industry has significant research and development capabilities. This tendency, based on certain tactical errors of the Russian armed forces in the first part of the war in Ukraine, is dangerous because it leads the population in Western countries to believe that Russia is not capable of dealing with a confrontation with NATO. In this context, it is necessary to correctly estimate the resilience of the Russian Federation's defence industry in order to take strategic measures to effectively counter a possible attack on a NATO or EU member state.

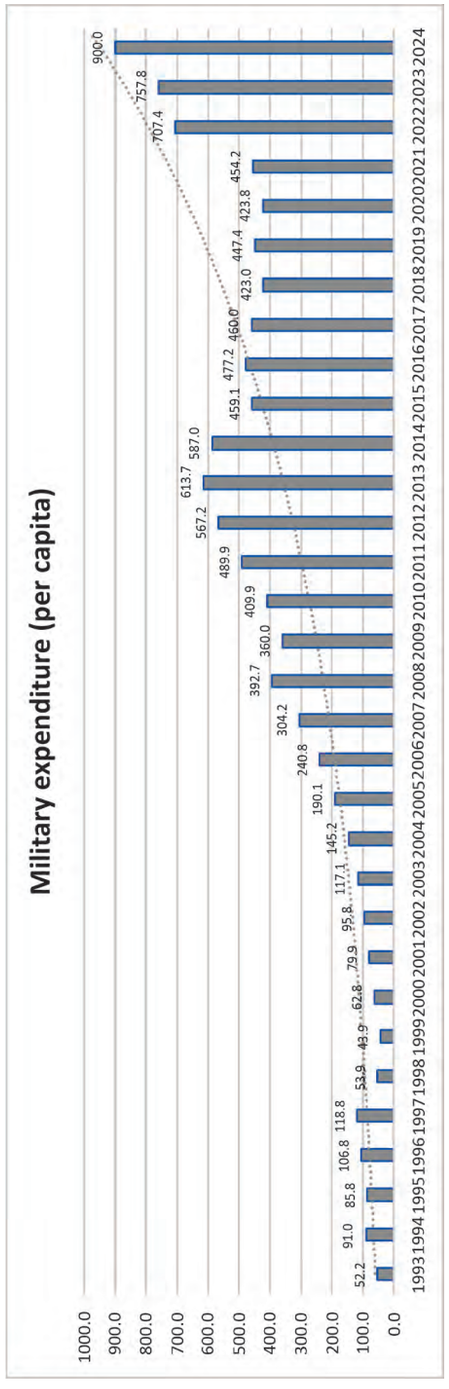
Similarly, if we look at the data on the nominal value of defence investments, we can see that they peak in 2024, a figure estimated by SIPRI specialists at USD 140 billion. An analysis of the data provided by SIPRI reveals that military spending in 2024 will have increased by more than USD 30,000 million compared to 2023, which once again reveals the Russian Federation's intention to continue the military conflict in Ukraine by providing its armed forces with modern weaponry and sufficient ammunition.



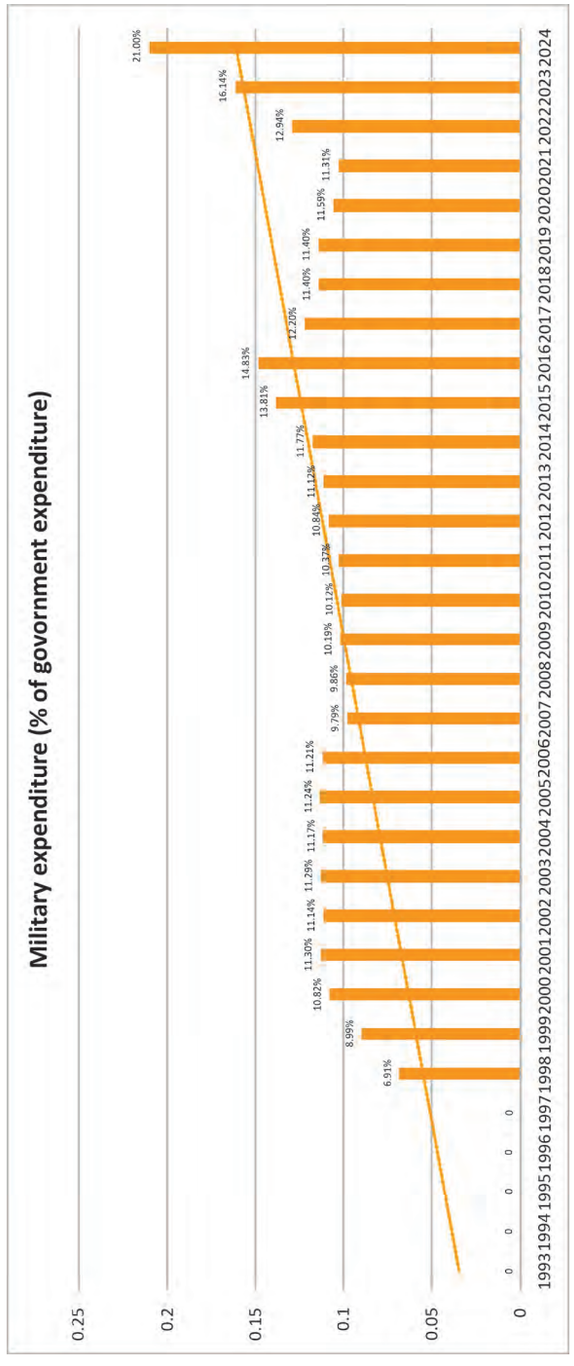
Graph 1: Evolution of the Russian Federation's defence resources allocation from GDP
(adapted from www.sipri.org)



Graph 2: Evolution of the Russian Federation's military expenditure (million USD) (lb.)



Graph. 3: Evolution of the Russian Federation's military expenditure (per capita) (Ib.)



Graph 4: Allocation of military expenditure of the Russian Federation (% of government expenditure) (Ib.)

The analysis of military expenditure per capita reveals a sharp upward trend from 2022 (the beginning of the military conflict in Ukraine) to 2024. Thus, it was recorded 707.4 USD/inhabitant in 2022, 757.8 USD/inhabitant in 2023, and an estimated 900 USD/inhabitant in 2024.

The analysis of military expenditures in relation to public expenditures of the Government of the Russian Federation reveals a higher allocation of funds in the period 2022-2024, with an estimated 21% in 2024, at the expense of other areas essential for the development of a given state (e.g. public health, education, social spending).

The Russian ground forces are still artillery-dominated forces, and the quantitative advantage in terms of ammunition and the number of artillery pieces available remains a critical factor on the battlefield. The Russian armed forces began the war with too few unmanned aerial vehicles (UAVs) and precision-guided munitions, meaning that it faced difficulties in accurately hitting certain military targets. This situation has changed, with the Russian Federation acquiring larger quantities of Orlan, Zala and Supercam series UAVs that provide persistent cover behind Ukrainian lines, while the widespread adoption of commercial UAVs (mainly DJI Mavics) has greatly improved frontline surveillance.

Krasnopol laser-guided artillery projectiles are also being used in larger quantities, along with Orlan-30 UAVs that can laser designate targets for artillery held by the Russian armed forces.

In conclusion, all the data presented above reveal the importance that the Russian Federation attaches to strengthening the Russian defence sector, i.e. the Russian military complex, with the aim of providing the Russian armed forces with the most modern military equipment at their disposal in order to gain a strategic advantage on the battlefield. Although Ukraine, through a sustained military effort, has entered the territory of the Russian Federation, the ability of the Russian Federation to regenerate certain armed forces and carry out counter-attacks with direct effects on the dynamics of the military conflict in Ukraine should not be underestimated.

SUPPLY OF MODERN MILITARY COMPONENTS TO THE MILITARY COMPLEX OF THE RUSSIAN FEDERATION

Lately, in order to avoid international sanctions imposed by Western states as well as the European Union and NATO, the Russian Federation has set up a mechanism that allows it to obtain the military and dual-use products and technologies necessary for the development of its own defence industry from states with which it has special economic and military relations (e.g. China, Islamic Republic of Iran, North Korea), especially China, a state that has advanced military technologies, given its willingness to invest large sums in military research. At the same time, the Islamic Republic of Iran has recently transferred short-range ballistic missiles to the Russian Federation for use in the war against Ukraine, finalizing a delivery that US and Western officials warned had been in the pipeline for almost a year (Petrescu, 2024). North Korea has exported to Russia the ammunition needed to support the war in Ukraine in return for the food supplied by the Russian Federation.

Russia is also smuggling military and dual-use components through illicit networks, mainly through the Eurasian Economic Union (EAEU), targeting mainly the Balkans, China, Türkiye and the Islamic Republic of Iran. This situation creates a form of parallel black-market economy for the supply of certain military and dual-use components, a market that helps sustain the Russian Federation's war economy (Miroshnychenko, 2023).

Despite the international sanctions imposed by NATO and the EU, the Russian Federation has demonstrated a continued ability to access sufficient quantities of Western military components by utilizing methods to circumvent international and national export control regimes. Adaptation to the current sanctions regime has been one of the strengths of the Russian military complex, constituting a serious warning to the effectiveness of the international export control system for military and dual-use goods and technologies (Ezhov, 2024). In this context, the Moscow authorities benefit from insufficient and inconsistent external enforcement of international sanctions, as well as from loopholes in the control of exports to third countries. Thus, the Russian Federation circumvents sanctions mainly through imports from third countries that are not part of the group of internationally sanctioned states (Bryne, Sommerville, 2023), namely China, the Islamic Republic of Iran, North Korea (through the notorious *"Orient Express"* ammunition supply routes), Türkiye, Kazakhstan, Belarus etc.

The above-presented aspects allow the Russian military complex to directly import certain commercially available systems (e.g. Iranian attack drones) and military components essential for the development of its own military equipment. The Russian defence industry also utilizes well-established networks of intermediaries that are not included on the international sanctions list, shell companies, entities disguised under other names in *"neutral"* states, the purpose of which is to import products and technologies for use by the Russian military complex (Corera, 2024).

In this context, it is necessary to consider the advisability of extending international sanctions also to those entities that support the acquisition of military and dual-use equipment necessary for the Russian military complex. At the same time, it is necessary to negotiate with the states which actively support the Russian military complex with equipment and ammunition in support of the military conflict in Ukraine, in order to reduce or even stop the aid granted to the Russian Federation.

In this regard, China, Türkiye and Kazakhstan are the main states that can agree to possible proposals to ban exports of military and dual-use products and technologies to the Russian Federation, given that certain commercial levers can be used in negotiations with these states. The other states, such as the Islamic Republic of Iran and North Korea, will not agree to exit their military relationship with the Russian Federation, given that the international community has imposed sanctions for violations of the non-proliferation regime for weapons of mass destruction and target-carrying missiles.

Currently, according to SIPRI, the Russian Federation has 5,889 nuclear warheads, of which 1,710 are ready for use and 2,670 are in storage (SIPRI, 2024).

In recent times, Russian officials have hinted at making changes to the Russian Federation's official stance on the use of nuclear weapons amid Ukraine's incursion into its border region of Kursk. These threats to use nuclear weapons are not unique, with Moscow officials continually threatening Ukraine and the West with the use of this type of unconventional weaponry.

Recently, Deputy Foreign Minister Sergei Ryabkov has said that Russia is in the process of amending its nuclear doctrine, which sets out the conditions under which nuclear weapons can be used, because of what the Russian Federation sees as a Western-backed *"escalation"* of the war with Ukraine.

The Russian Federation has accused the West of encouraging Ukraine's cross-border raid, which has seen Ukrainian armed forces seize almost 800 square kilometres of Russian territory since it began on 6 August 2024. Ukraine's NATO

allies deny any prior knowledge of the operation or direct or indirect participation in the offensive. All these considered, it is possible that NATO member states were not aware that Ukraine had used Western weaponry in the attacks on Russian territory.

In this context, the Deputy Foreign Minister of the Russian Federation has said that work is *"at an advanced stage"* on amending the nuclear doctrine governing the use of nuclear weapons. Currently, the nuclear doctrine states that the Russian Federation *"reserves the right to use nuclear weapons in response to the use of nuclear weapons and other types of weapons of mass destruction against itself and/or its allies, as well as in case of aggression against the Russian Federation with conventional weapons, when the very existence of the state is threatened*". Other conditions that could trigger the use of nuclear weapons by the Russian Federation include *"receipt of reliable intelligence on the launch of ballistic missiles attacking the territory of the Russian Federation and/or its allies"*, as well as *"enemy impact on state or military facilities of critical importance"* (Ib.).

While Russia's threats to use nuclear weapons are nothing new, Ryabkov's comments, which follow recent statements by high-ranking officials, including at the level of the Presidential Administration, indicate that the Russian Federation is preparing the ground for changes in state policy on the conditions under which the use of nuclear weapons would be acceptable.

Ukraine's incursion into Russian territory and its targeting of military facilities and infrastructure with Western-supplied weaponry, particularly long-range missiles, has also raised the stakes as to whether Moscow might consider using nuclear weapons to defend its own territory.

In this context, the possibility of a tactical nuclear weapons attack by the Russian Federation against Ukraine should not be ignored, with the capital Kyiv as a potential target. The choice of the capital lies in the fact that a tactical nuclear strike must have a major psychological impact and lead to the urgent start of peace negotiations on terms favourable to the Russian Federation. So far, the Moscow authorities, although they have repeatedly threatened the use of nuclear weapons, have refrained from using them in view of the potential military and strategic repercussions, through the imposition of drastic political and economic sanctions by Western states and international organizations (e.g. the UN).

A nuclear-weapon attack by the Russian Federation against a NATO or EU member state is highly unlikely, given the immediate military consequences and the possibility of similar attacks by NATO, with uncontrollable security effects.

POSSIBLE IMPLICATIONS FOR ROMANIA OF THE MILITARY ACTIONS CARRIED OUT BY THE RUSSIAN FEDERATION

The military conflict in Ukraine is located at the state border of Romania, our state being affected by an important influx of refugees from the start of the war until now. The Romanian authorities have ordered effective measures for the proper management of this flow of refugees, the efforts made by the state institutions being appreciated by the leading factors of the European Union and NATO.

A major risk is represented by the military actions of the Russian Federation which at one point aimed to conquer the city of Odesa and its surroundings. There is a risk that in the situation where the Russian armed forces succeed in conquering this area, we will have a common border with Russia. A risky situation was represented by the conquest of Snake Island by the Russian armed forces at the beginning of the war, an aspect that generated a strategic position of the Russian Federation in the proximity of the territory of Romania. Snake Island constitutes a strategic position in view of the fact that the Russian armed forces could more easily monitor the movements of national and NATO troops positioned in the Dobrogea region.

Another risk factor is represented by Russian drones that fly over the territory on the border between Ukraine and Romania, and there have been incidents when fragments from Russian drones have been identified on the national territory. Also, another risk factor is represented by the bombings of the Russian armed forces in the Ukrainian ports located in the immediate vicinity of the state border of Romania, as there is a risk that certain shells accidentally reach the national territory.

The nuclear danger must not be excluded, as it is represented, mainly, by the danger generated by incidents generated deliberately or accidentally at the level of the Zaporozhe Nuclear Power Plant (NPP), which is currently under the control of the Russian Federation. In the event of a radiological incident at the Zaporozhe NPP, there is a risk of radiological pollution of the national territory, similar to the period after the nuclear accident occurred in 1986 at the Chernobyl NPP, affecting the health of the Romanian population and the national economy.

Also, although the probability is very low, there is a risk of an attack by Russia with tactical nuclear weapons against Ukraine. In this context, there are consequences regarding radiological damage to the population of Romania. A nuclear attack by the Russian Federation affecting a NATO member state is extremely unlikely, given

the effects on Russia that will be immediately implemented by the North Atlantic Alliance.

Considering these aspects, it is necessary to speed up the modernization process of the Romanian armed forces at the national level, including by increasing the budget allocations dedicated to the modernization of the defence industry and for the purchase of modern military equipment from the foreign market. At the same time, it is necessary to act for the recruitment of properly trained military personnel to face a possible modern war, including the training of reservists who can support the professional armed forces in the event of a military conflict triggered by the Russian Federation.

At the same time, the hybrid actions carried out by entities directly or indirectly coordinated by the Moscow authorities should not be neglected, such as disinformation campaigns and cyber attacks against the websites of the Romanian authorities or those related to critical infrastructure. In this context, it is necessary to combat disinformation to carry out an effective strategic communication by the institutions of the National Security System. In the case of cyber attacks, the level of training of specialized institutions that are able to prevent such attacks or limit their effects to a minimum at the level of the essential institutions of the Romanian state must be increased.

CONCLUSIONS

The analysis shows that the Russian Federation armed forces are capable of facing opponents of the same level. The fact that the authorities in Moscow do not take into account the human and material losses on the front makes the Russian Federation a dangerous adversary, even for more technologically advanced adversaries (e.g. the USA). Also, another advantage of the Russian Federation is given by the nuclear arsenal at its disposal, the authorities in Moscow being willing, under certain conditions, to use this arsenal by assuming any security consequences.

In this context, it is necessary that not only at the level of NATO and the EU, but also at the level of the member states, individually, to continuously monitor the defence industry of the Russian Federation, with an emphasis on the development of capabilities that can be used for a possible attack of the member states of NATO and/ or the EU. In this regard, it is necessary to anticipate future trends in the field of the defence industry, with an emphasis on the ability of the Russian Federation

to regenerate the armed forces, the structure of the forces, their command and control. Another very important aspect of the research is the analysis of the challenges and opportunities facing the Russian Federation in terms of production/ procurement of state-of-the-art military equipment and technologies.

This analysis can also be used to correctly assess the effects of the sanctions imposed at the level of the Euro-Atlantic organizations against the Russian Federation, as well as the effectiveness of these measures. After carrying out a relevant assessment, other sanctions can be adopted or the existing ones can be updated, including by taking sanction measures against states that support the military complex of the Russian Federation, even through the delivery of military equipment or strategic materials from Western states that reach Russia through intermediate companies specialized in circumventing the export control regime of military and dual-use products and technologies.

BIBLIOGRAPHY:

1. Bermudez, J.S., Cha, V., Jun, J. (6 October 2023). *Dramatic Increase in DPRK-Russia Border Rail Traffic After Kim-Putin Summit*. Beyond Parallel, https://beyondparallel.csis.org/dramatic-increase-in-dprk-russia-border-rail-traffic-after-kim-putin-summit, retrieved on 8 September 2024.
2. Bilousova, O., Gribanovskiy, O., Hilgenstock, B., Ribakova, E.&Shapoval, N., Vlasiuk, V. (June 2023). *Russia's Military Capacity and the Role of Imported Components*, https://kse.ua/wp-content/uploads/2023/06/Russian-import-of-critical-components.pdf, retrieved on 8 September 2024.
3. Byrne, J., Somerville, G. (2023). *The Orient Express: North Korea's Clandestine Supply Route to Russia*. Report. London: Royal United Services Institute, https://rusi.org/explore-our-research/publications/commentary/report-orient-express-north-koreas-clandestine-supply-route-russia, retrieved on 8 September 2024.
4. Corera, G. (21 February 2024). *Russia 'Struggling with Supply of Weapons and Ammunition' for Ukraine War – Western Officials*. BBC, https://www.bbc.com/news/world-europe-68364924, retrieved on 8 September 2024.
5. Ezhov, S. (27 January 2024). *Our man in Brussels: The Insider has unmasked GRU officer helping the Kremlin evade sanctions from his base in the heart of Europe*. The Insider, https://theins.ru/en/ politics/268669, retrieved on 8 September 2024.
6. Miroshnychenko, B. (29 May 2023). *Russia's military-industrial complex is gaining momentum. Where does the money come from, and who helps Russia produce missiles?* Ukrainska Pravda, https://www.pravda.com.ua/eng/articles/2023/05/29/7404294, retrieved on 8 September 2024.
7. Petrescu, E. (2024). *Iranul i-a trimis Rusiei rachete balistice. Dezvăluiri din presa americană care alarmează Washingtonul*, https://ziare.com/razboi-ucraina/iran-rachete-balistice-rusia-1892509, retrieved on 8 September 2024.

8. SIPRI (2024). *Role of nuclear weapons grows as geopolitical relations deteriorate*, https://www.sipri.org/media/press-release/2024/role-nuclear-weapons-grows-geopolitical-relations-deteriorate-new-sipri-yearbook-out-now, retrieved on 8 September 2024.
9. Trevelyan, M. (2024). *Russia says it will change nuclear doctrine because of Western role in Ukraine*, https://www.reuters.com/world/europe/russia-will-change-nuclear-doctrine-due-wests-actions-ukraine-official-says-2024-09-01/, retrieved on 8 September 2024.

DIRECTED ENERGY WEAPONS – COMPONENT OF DISRUPTIVE EMERGING TECHNOLOGY WITH IMPLICATIONS ON STRATEGIC STABILITY –

Colonel (r.) Romică CERNAT, PhD
Visiting Professor, Department of Political Sciences, Faculty of Political Sciences, Philosophy and Communication Sciences, Western University, Timișoara
DOI: 10.55535/RMT.2024.4.39

Directed energy weapons represent an emerging, disruptive, credible, relevant technology with the potential for use in all military action domains and with the role of influencing the power balance globally.

Given that the nature of the threats has changed in the current security environment, the great powers need a more strategic approach to capitalize on future technologies, including directed energy weapons, in a successful manner. Against the background of escalating tensions in many regions of the globe, emerging technologies are an essential lever for both defence and deterrence. In relation to conventional kinetic weapons, directed energy weapons have some advantages – precision, reduced costs, calibrated effects, possibility to be employed to neutralize vital targets for adversaries without causing collateral damages –, but also some disadvantages: decreasing the force and effect of the radius/beam, relatively range short, impossibility of being employed against the targets located behind some obstacles, low progress in adapting to the needs of the armed forces services and fielding in weapon systems.

Electromagnetic radiation is critical for communications, command and control, navigation, targets acquisition, information collection, surveillance, reconnaissance, missile guidance, early warning, and neutralization of targets, aspects that have propelled the development of capabilities, including directed energy weapons directed, to counteract efficient use of electromagnetic spectrum or to neutralize some targets.

Keywords: directed energy weapons; high energy lasers; high-power microwave weapons; electromagnetic spectrum; drones;

INTRODUCTION

The shifting of world order and the largest technological competition of the last era are in progress. It is increasingly difficult for a superpower to maintain technological supremacy considering the ascension and progress of China but also the technological evolutions of the other great powers. Russia and China, along with their allies, make visible efforts to reorganize the world order and promote their global economic and political interests – actions that threaten the USA status as a global leader (Booz, 2024, pp. 1-10).

Several *emerging technologies* are mentioned in the documents on US national security and the studies on the balance of power and deterrence at the global level. They could have a disruptive impact on the two fields in the coming years as well as significant implications for the arms race, the military concepts of operations, and the future of the war. These technologies include: *artificial intelligence, lethal autonomous weapons systems, hypersonic weapons, directed energy weapons, biotechnology, and quantum technology.*

Directed energy weapons (DEW) are defined as those weapons that employ concentrated electromagnetic energy, to prevent normal functioning, cause physical damage, disable, destroy the equipment, technique, and armament as well as to neutralize the enemy personnel. The *reduced costs* for shots and the *almost unlimited ability to execute fire* transform them into efficient and effective assets, in relation to the conventional ones, to defend against volleys of missiles, and large and dense air group unmanned vehicles.

Theoretically – due to reaction speed – the directed energy weapons could represent a viable option for missiles interception in the boost phase, but experts are not convinced of the feasibility and implementation of this solution. DEW could be employed to temporarily disable or damage the satellites and sensors, an action that could affect intelligence collection operations, military communications as well as the positioning, navigation, and synchronization systems utilized to determine targets. *High-powered microwave weapons (HPMW)*, as part of DEW, *represent non-kinetic means for neutralizing communication and electronic systems, as well as improvised explosive devices.* Also, the possibility of using them for crowd control has been explored (Sayler, Jan. 2024, pp. 1-3, O'Rourke, 2023, pp. 1-20, Sayler, Feb. 2024, pp. 1-3).

We are in a period of an increased competition for superpower status that has as consequence an increasingly challenged security environment, with wars in Europe and the Middle East as well as confrontations in the South and East China Seas. The USA assesses China as the main threat to its national security, closely followed by Russia. Lately, both have supported a large program of investment in science and military technology. China, in order to counteract the US Joint All-Domain Command and Control initiative/JADC2, develops a new military project known as *Multi-Domain Precision Warfare* to modernize its every domain-specific force, from the cyber to the space. Both fundamental operational concepts are based on the interconnection of command and control, communications, computers, intelligence, surveillance, and reconnaissance to quickly coordinate the fire power and exploit the weaknesses of the opponent. The analysts in the defence area claim that DEW will play a key role in what is known as *stratified defence,* having the technology or countermeasures to neutralize multiple threats in complex situations. The implementation of DEW is affected by their technological complexity but also by certain materials, such as germanium and gallium, and the expensive precision components (Demarest, 2024, pp. 1-5).

DEW include *high energy lasers* (HEL), *high-power microwave weapons* (HPMW), and *particle beam weapons* (Sayler, Feb. 2024, pp. 1-3). DEW are part of a set of advanced capabilities and domains that are essential for *deterrence* and *maintaining the competitive advantage* by the great powers. This article analyses some of the consequences of introducing these weapons in equipping the armed forces for global stability (Townshend, 2019, pp. 2-15; Department of Defense, 2022, pp. 1-22).

Emerging technologies are effective for deterrence when potential opponents are provided with sufficient data on a particular system of weapons, to consider it certain, and authentic, and simultaneously, they create uncertainty about the potential of their capabilities (Townshend, 2019, pp. 2-15). The Ukraine conflict has also highlighted a change in the strategy of the great powers generated by the employment in all domains of a broad spectrum of weapon systems and platforms, from conventional to capabilities based on emerging technologies, political and informational war, cultural tools, and sophisticated forms of exercising of power. *The power projection based on the association/combination of the new emerging technologies with the latest hybrid warfare techniques and ambiguous challenges and thresholds determine a new dimension of deterrence*. Adapting to these new realities by adopting effective and firm approaches to this type of deterrence

could be a way of response (Ib.). A new generation of weapons – many based on so-called emerging technology – will enable the forces deployed in the theatre of military actions to discover and strike the targets, timely, precisely, and quickly in all domains of waging battle actions.

The great powers allocate considerable funds to developing DEW – critical and emerging defence technologies – to employ them to overcome the threats presented by drones and rockets but also for use as space-based capabilities. Among the potential applications can be mentioned *HEL* and *HPM, short-range air defence systems (SHORAD) to neutralize unmanned aerial systems (UAS)*, as well as *rockets, artillery, and mortars (RAM)* (Demarest, 2023, pp. 1-12). *NATO has accelerated the transformation and adaptation process to meet current and future threats and maintain technological advantage, including experimentation and more rapid fielding of emerging technologies*. (North Atlantic Council, 2024, pp. 1-6).

The *laser* uses the directed energy to neutralize a target. It is not achieved by heating and melting, there is no reciprocal action of waves, but only a large amount of energy. A beam or energy beam is focused to blind, cut, or cause damage by heating a target. The HPMWs use the electromagnetic spectrum in the air, and space to cancel/stop the ability to operate properly of any system that uses voltage and current. They emit waves of energy that overload or *"fry"* electronic components. Each type of directed energy weapons has *strengths* and *weaknesses*. For a laser to be effective, its system must be able to detect a threat and track it. Even if they are powerful and practical, and the system has relatively small dimensions, the estimated distance at which the current systems operate is approximate 7 kilometres (Demarest, ib.). Moreover, weather conditions and duration of action can still affect their effectiveness. While HPMWs can have a practically instant effect on electronic components, their effectiveness is reduced at greater distances. While HELs can drill different materials, certain atmospheric conditions, including fog or wind, can affect or change the target's result. Given that everything is automated, the platform is dependent on the production, continuity and amount of electricity that supplies it. The armed forces make efforts to materialize the directed energy systems in offensive and defensive capabilities.

In the defence community, it is generally recognized that there is a great gap between the *technology's development, fielding and its acquisition*. Regarding the directed energy weapons – too important technology to be ignored, according to experts – there is a pressure and emergency for acceleration, generated by the Ukraine war, for the necessity to complete the development and implementation

process (Ib.). Due to the explosive development of modern technology and accelerated proliferation of armaments, there is a real concern among scientists regarding the effects of science and technology on mankind, positive and negative, potential and real, and especially regarding the role of science and scientists in the balanced evolution of implementation of their results in the military field. As the conflicts in Ukraine and the Middle East continue, the great powers act to make the armed forces suitable for the new reality of warfare and streamline the modernization strategies to cope with the challenges of conducting fighting actions in different domains (Demarest, 2024, pp. 1-5).

Global stability, as a rule, is affected when a great power has military capabilities and the other great powers still do not have the necessary capabilities to counteract them, or a great power can obtain an obvious advantage by triggering a war. If we consider the USA, China, and Russia, the global system will be unstable when, by a first strike, one of these great powers has the capacity to eliminate the entire response capacity of the other. In this situation, none of the parties would have any reason not to initiate the first nuclear strike, but at the same time, each party knows that any total war will produce massive damage, no matter what triggered the first strike, so the situation is relatively stable. The paradoxical consequences of developing weapons that use emerging technology is that the destructive effects on personnel and equipment or the danger of triggering a war are, apparently, reduced, but, in reality, mankind is moving to a volatile and hazardous world (Gertler, 1987, pp. 1-2, 5-15).

DEWs have the potential to change the way of conducting military actions and the nature of warfare, which will have consequences for the national security of the great powers. These implications, among others, refer to: *decreasing the duration from the sensor to the shooter, engaging more targets before the adversary can take action, as they can be used as a sensor and as a weapon; DEW contribute to achieving air supremacy by neutralizing enemy air defence; DEW rapidly locates and attacks the surface-to-air mobile systems*. HPMWs represent antiradiation attack capabilities, deny anti-detection actions, and measures of enemy air defence systems, and attack them by turning off their systems; they can be employed in effects-based precision operations by counteracting the most problematic asymmetric strategies utilized by the enemy: the use of civilians as shields, without hurting civilians in the area; DEW can contribute to limited space control. For defensive purposes, it ensures the security of their own space-based assets, for offensive purposes, it may temporarily deny the employment of the enemy space-based capabilities

and the damage or destruction of enemy satellites (Feickert, 2018, pp. 1-29). DEWs represent an operational advantage source for the owner state of such weapons and then these emerging technologies, once fielded, have the potential to influence the balance of global power. Concerning other capabilities, DEWs have a unique essential characteristic that provokes precise and calibrated effects against multiple targets almost instantaneously at a very low cost with high operational efficiency (Gunzinger, 2012, pp. pp. xiii, 1, 20-28).

Directed energy battle actions are *military actions that entail the use of weapons, devices, and countermeasures with directed energy to incapacitate, provoke direct damage, or the destruction of enemy equipment, technique, and armament as well as the neutralization of the personnel or to interrupt, exploit, decrease or prevent hostile employment of electromagnetic spectrum (EMS) through damage, destruction, and disruption*. They also include actions undertaken to protect friendly equipment, facilities and personnel, and to maintain the employment of their own EMS. These are part of the electronic warfare missions and encompass active technology denial, lasers, radio frequency weapons, directed energy anti-satellite systems, and HPMW systems. (Defense Intelligence Agency, 2022, pp. 41-48, Gunzinger, ib.).

Directed energy (DE) is an expression used to ***depict an extensive range of non-kinetic capabilities that produce a beam of concentrated electromagnetic energy or atomic or subatomic particles capable of damaging or destroying enemy equipment, facilities, and personnel in all battle action domains***. ***Directed energy battle actions*** comprise actions taken to ***protect the own forces' equipment, facilities and personnel, and to secure the employment of the electromagnetic spectrum by friendly forces*** (Gunzinger, ib.). The armed forces that develop and field battlefield lasers and HPMW will possess a noticeable military benefit. DEW will complement kinetic weapons and combat emerging threats like drones, fast attack boats, and cruise missiles. Details are provided in *figure 1, 2* and *3*. In *figure 1* incoming drones and missiles are depicted (Demarest, 2023, p. 4).

Some analysts claim that the potential of DEW could change the very nature of war or could ensure states that own such weapons an undeniable advantage, while others emphasize that laser-based projects have not developed at the forecast pace (Feickert, 2018, p. 5).

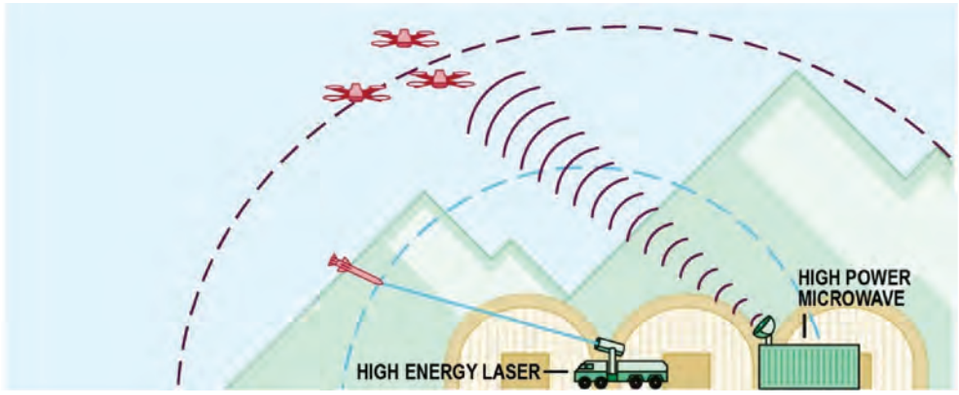


Figure 1: The way in which directed energy weapons can be used in combat (Demarest, 2023, p. 4)

THE LASER – FEATURES, EMPLOYMENT IN BATTLE ACTIONS

HELs use concentrated light to inflict physical damage on a target. By fielding viable weapon systems, DEW has a potential significance in tackling current and emerging threats to neutralize missiles, artillery and mortars, in eliminating certain threats to air defence against short-range assets, and in obtaining success in fighting actions in all domains (O'Rourke, 2023, pp. 1-20). Airborne HELs can potentially transform the nature of the battle in all domains. Aircraft or platforms equipped with HEL can be used for striking ballistic missiles, surface-to-air missiles, unmanned combat air vehicles, surface craft and other air platforms as well as space-based systems and can be successfully employed in carrying out precise strikes on particularly enemy targets extremely defended and also for surface-ships self-defence or ground forces equipment (O'Rourke, 2024, pp. 1-20)

Electromagnetic spectrum. *The electromagnetic spectrum (EMS)* is *the range of wavelengths or frequencies of electromagnetic radiation. It includes radio waves, microwaves, visible light, X-rays, and gamma rays*. As the wavelength of the electromagnetic radiation shortens, the waves have a higher frequency – how quickly electromagnetic waves follow each other – and therefore more energy *(figure 2)*. These waves are called *electromagnetic waves* because they have both electric and magnetic properties. Such waves vary in frequency, wavelength, and energy. Scientists classify electromagnetic waves by their wavelength or frequency. Waves with shorter wavelengths (e.g., gamma rays) have higher frequencies and higher energy; waves with longer wavelengths (e.g., radio waves) have lower frequencies and lower energy (Hoehn, 2022, pp. 1-3). In the military field, most of the communication equipment is based on radio waves and microwaves,

and infrared and ultraviolet spectrums are used for laser technologies and intelligence collection. Infrared and ultraviolet lasers have a greater bandwidth than radio frequencies and allow the dissemination of large volumes (for example, video) for long distances due to signal power. In the military field, lasers can be used as offensive means, to temporarily blind the satellites' sensors, destroy drones, and for other purposes (Sayler, 2021, pp. 1-21).

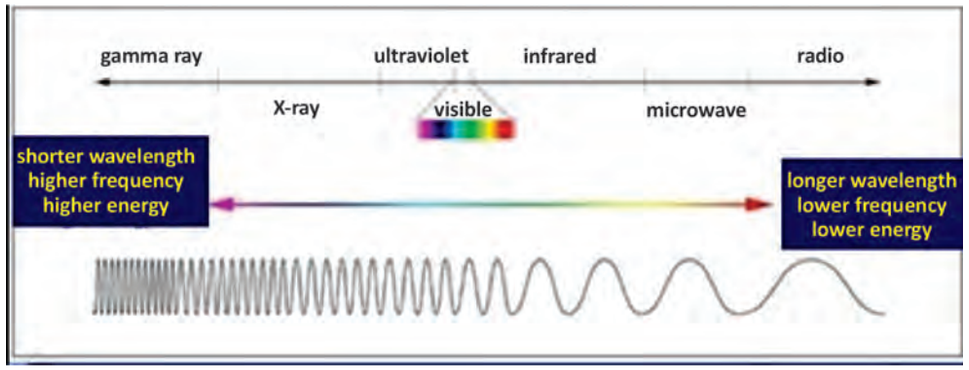


Figure 2: The electromagnetic spectrum (Hoehn, p. 1).

Current military applications of the spectrum. Almost all modern weapon systems, such as those used by aircraft, satellites, terrestrial battle equipment, ships, and radio stations, depend on the spectrum to operate. EMS is also used for: ***Communications*** – data transmission almost instantly between the elements of the elements of the battle array, by using the terrestrial radio stations and the communication satellites; ***Situational awareness*** – the use of radio waves, microwaves and infrared radiation to develop a picture of the battle space, by determining the location of the own forces and the enemy ones. The most common situational awareness applications: passive radar (LIDAR – ***light detection and ranging***), detection and collection of spectrum emissions (SIGINT), infrared sensors; ***electronic warfare*** – the use of EMS to gain and maintain its operational control; ***spectrum operations*** – command and control (C2), signature management (manipulate the spectrum to reduce the electromagnetic signature, and identify and neutralize forces) and navigation warfare (deliberate offensive and defensive actions for efficient use of positioning, navigation and timely use of information simultaneously with denying these actions for the adversary by coordinated employing of space-based, cyberspace and electronic warfare capabilities), command and control and especially for ***Emerging Military Applications***

of the Spectrum (fifth generation – 5G – of communications, use and Applications of Artificial Intelligence, DE technologies-laser communications, DEW, Counter-UAV) (Sayler, 2021, pp. 4-19). *Electronic warfare*, defined as *military activities that use electromagnetic energy to control the electromagnetic spectrum ("the spectrum") and attack an enemy* (Hoehn, 2022, pp. 1-3). Some programs aim to make lasers to solve the capabilities gap to address asymmetrical threats – unmanned aircraft (UAV), small boats, and information, surveillance, and reconnaissance sensors.

The laser *uses electricity to generate photons or light particles*. The photons pass through an amplification medium – an amalgam of substances – that rapidly develop many photons, all having the same characteristics as the initial photon. This fact determines the coherence feature of laser beams – to finally focus on a narrow beam (Boyd, 2024, pp. 1-3). The high-energy laser systems – used in the military field – are based on solid-state lasers that use special crystals to convert the input electrical energy into photons. The main feature of high-power solid-state lasers is that the photons are generated in the infrared segment of the electromagnetic spectrum and, consequently, cannot be seen by the human eye (Gunzinger, pp. 20-28).

HEL Weapons, Potential Advantages and Limitations

The ***main advantages*** are represented by: *the low cost per shot*; *a huge number of shots*; and *the rapid target engagement time*, the light from a laser beam can almost instantly strike a target, causing the target damage in seconds, after which it can immediately engage another target; *the capacity to counteract the guided missiles*, by tracking and maintaining the beam on the missiles*; the precision target engagement*, the laser spotlight emitted can have a several- centimetre diameter and damage only what strikes without collateral damage and calibrated responses, can achieve other effects than the destruction of targets, namely the targets' detection and monitoring or causing non-lethal effects such as the reversible blockage of the electro-optical sensors.

The ***potential limitations*** of the lasers refer to*: the line of sight*, the laser light moves through the atmosphere on a straight trajectory, thus limiting their range. Only the targets located up to the horizon line or those that are not protected by certain shelters will be employed; *atmospheric absorption, dispersion, and turbulence*, the substances in the atmosphere can affect the laser's quality, efficacy, and range. Absorption increases proportionally, in general, with target distance. Rain or fog can prevent the normal functioning of the lasers; *thermal blooming*.

A laser system that engages the same target for a longer period can heat the air through which it passes, this phenomenon alters the quality of the laser beam and reduces the effect on the target; *saturation attacks.* A laser can engage a single target simultaneously, it requires a few seconds to be turned off and redirected to the next target. This determines the maximum limit of targets that can be engaged in a period; *hardened targets and countermeasures*. Lasers with smaller beam powers measured in kilowatts may have a lower efficacy against shielded targets, from ablative material or extremely reflective or rapidly rotating as well as targets using masking measures; *risk of collateral damage to aircraft, satellites, and human eyesight*. The laser radius with ascending orientation, which does not strike the target, continues its movement, with the risk of hitting aircraft, radars, sensors, or satellites and provoking unwanted collateral damage. Light issued by lasers on certain frequencies can cause permanent damage to human eyesight, including blinding. (O'Rourke, 2024, pp. 3-27; 2023, pp. 1-20). The effects of weapons with HEL compared to those with HPM are presented in *figure 3*.

Numerous ***military applications*** use HELs. Among them can be listed: lasers in the infrared and ultraviolet ends of the spectrum to dazzle satellite sensors and destroy drones; the use of emerging communications technologies of lasers – transmitting light, instead of radio waves, between antennas; the use of lasers to disable intelligence collection sensors, destroy small UAS and satellite communications; precision-guided munitions use laser guidance to improve a weapon's accuracy to less than 3 meters (Lucas*,* 2022, p. 1); the development, procurement, and fielding/deployment of high-energy laser weapon systems to counter, destroy UAS – low, slow, small – usually called drones; in covert and clandestine operations for identifying personnel at distances of around 200 meters (Sayler, 2023, p. 1); there is no consensus on the level of precise power that would be needed to neutralize various target sets, certain documents claim that: lasers of around 100 kW (Sayler, 2024, pp. 1-3) could engage unmanned aircraft systems, small boats, rockets, artillery, and mortars, whereas lasers of around 300 kW (Ib.) could additionally engage cruise missiles flying in certain profiles (i.e., flying across – rather than at – the laser), to defend fixed or semi-fixed critical assets against cruise missiles, unmanned aircraft, missiles, artillery, and mortars. Lasers of 1 MW could potentially neutralize ballistic missiles and hypersonic weapons – at a range of up to 20 km; weapons to disrupt, degrade, or damage space-based satellites and their sensors on a low orbit including non-optical satellites; ground-based laser weapons that can damage space-based sensors on a low orbit; higher power

laser systems that can degrade non-optical satellites; destructive capabilities that use the laser to disrupt space-based weapons; laser-guided rocket systems; 50-kw laser weapons to defend against air and artillery threats; indirect fire protection capabilities; light detection and ranging – LIDAR is a remote sensing method that uses pulsed laser light to measure the distance, speed, and/or altitude of physical objects to map the surrounding environment. LIDAR allows for precise, accurate, and rapid three-dimensional measurements of natural and artificial environments, with high resolution and long-range detection; LIDAR can also be used to identify and determine the depth of the coast mine fields and for atmospheric monitoring; more powerful laser on the surface shipboard of the navy to counteract a wide range of surface and air targets at ranges up to about 20 km. (Hoehn, pp. 1-3, Sayler, 2024, pp. 1-3, O'Rourke, 2024, pp. 18-21).

Lasers ***are classified*** by the *gain medium* used for light amplification: *with gas-neon helium* for metrology applications, carbon dioxide for material processing; *a semiconductor (diode)* – that contains a semiconductor positive- negative junction. They are the most effective regarding the power-to-cost ratio, high power conversion efficiency, high quantum efficiency, and a wide range of available wavelengths. They are used in telecommunications, materials processing, bar code scanning, medical lasers and LIDAR systems; and, *solid-state lasers* – which use crystals or glass materials doped with transition metal or rare earth ions. They can reach the highest powers from all available lasers and are used for material processing, medical, and military fields (Edmund Optics, 2023, pp. 1-3). *Solid-state lasers* developed for potential use in different environments: *fibre solid- state lasers* fuelled by electrical power, *slab lasers*, and *free electron lasers*. All three types are electrically or chemically powered. At the navy, the existing electricity system on the ship is used (O'Rourke, 2023, pp. 9-14). The increasing use of laser capabilities within the integrated anti-aircraft and missile defence systems is obvious, most likely in the lower level as an altitude of target employment.

For now, DEWs are best suited to fight UAV. The use of laser weapons could be an alternative, less expensive, to rockets-based defence, which can be overwhelmed by multiple targets, against scenarios with small and cheap drones that fly in swarms at low altitudes.

HIGH-POWERED MICROWAVE WEAPONS – FEATURES, EMPLOYMENT IN BATTLE ACTIONS

High-powered microwave weapons, which are part of directed energy weapons, can be used as a non-kinetic means of disabling electronics, communications systems, and improvised explosive devices or as non-lethal *"heat rays"* for crowd control (Sayler, 2021, pp. 1-21). Details are found in *figure 1, 2* and *3*. Conflicts in Ukraine and Israel provide sufficient evidence of the opportunity to neutralize the autonomous drone swarms – asymmetric capability – with low costs, employing non-kinetic weapons, namely HPM.

There are programs for the development of ***two types*** of weapons using HPMs: HPMWs with ***continuous and pulsed waves***. *Continuous wave* HPMWs emit a constant flow of microwave energy in a wide area and can be used in area denial operations against personnel or small electronic devices, such as UAS. *Pulsed wave* HPMWs emit high-power, short-duration pulses of microwave energy, within a wide range of frequencies, from 1 megahertz to 100 gigahertz, and can ensure precise targeting. The weapons that use HPM with a pulsed wave employ a set of specific targets to destroy or degrade their electrical components. ***Knowing the frequency of the target is mandatory*** to determine the energy needed to penetrate the electronic components and obtain the desired effect. The transfer of energy to the receiver/target is determined by the overlap of frequencies, that is, if they are in-band or out-of-band. The amount of energy getting to the target is affected by the way the energy propagates through the atmosphere. The transfer using a narrow band provides a higher amount of microwave energy to the target, but the coupling is harder. In the past twenty years, the HPMW energy sources have evolved, the weight has been reduced and the power of microwaves has increased. In 2003, a 400-kg device produced 20 gigawatts of power and now could produce terawatts of energy making it possible to install these systems on smaller platforms. It has also evolved the distance from which HPMWs can successfully engage a target, from several hundred meters in 2002 to a few kilometres now (McGonegal, 2020, pp. 3-15). Significant progress has been made, particularly by the United States of America, Russia and, China in the development of these weapons. HPMW, due to the high microwave power to be transmitted, are not sufficiently effective at ranges much greater than a few kilometres.

The HPM devices, according to the size of the band they emit, can be classified into two types: ***ultra-wideband*** (UWB), which operate high voltage spikes in impulse-configurated, linked or connected with an antenna to radiate on the range of preferred output frequency; and with ***narrow band***, which operate an electron

beam to emit high power radio frequency signals at a particular band frequency. Because the energy is distributed throughout the entire bandwidth, there is a reduced probability that the ***UWB*** sources have the power to damage a device. In a narrow band device due to the ***narrow bandwidth***, there is a risk that the target frequencies do not overlap with the device bandwidth or the target has a strong shielding for the frequency band used by the device, and ultimately the target is not neutralized. Given the complexity of the target shielding, the HPM devices represent effective assets for neutralizing electronic devices (Green, 2022, pp. 71-73).

Among the goals of ***military applications*** using HPMW can be listed: to defend aircraft against surface-to-air missiles; relevant enhancement of the antiradiation attack capabilities and counteracting the enemy air defence systems actions to avoid detection and attack by turning off their systems; neutralization of WMD facilities that are sheltered, fortified or placed near areas with population or civil infrastructure; engagement in conducting precise effects-based operations; they can practically attack any electronic system without doing direct harm to civilians near the targets; disruption of the electricity production and distribution in the short term or the destruction of subsystems; the conduct of strategic strikes against industrial systems and military infrastructure, dependent on electricity and electronic systems; for offensive purposes, they can temporarily deny the employment of space-based assets by opponents and cause the destruction of enemy satellites (Feickert, 2018, pp. 1-29; Walling, 2020, pp. 11-17).

Some studies contend that HPMW can damage computer networks, neutralize drones, swarms of drones, and missiles. At the same time, they can be used effectively against mines and minefields, especially intelligent mines. Analysing microwave sources with different output spectra has showed that narrowband sources are more effective, but broadband sources are preferred to excite resonances in electronic packages. All types of HPM devices use a source of pulsed power, on which the effectiveness in battle depends. The delivery of HPM to the target can be done using fixed assets, which do not involve complex technologies or miniaturization of critical components (antenna and the source) so that it can be transported to the target with the help of a missile (Green, pp. v- vi).

The power source of HPMW can be placed on cruise missiles, but also on the aircraft, to transport and launch them. The missile trajectory and target list are scheduled before taking off the aircraft that is launching these missiles. Once launched from the aircraft, the missile will fly the payload – HPM – on its pre-programmed trajectory, enabling it to strike the planned target. Each weapon that employs HPM realizes effects on the target, but the way and the means with which HPM will be

transported to the target are diversified, including autonomous systems. The HPM technology will evolve by creating several options to mount this technology on different, new, or old platforms to become a feasible technology. The effectiveness of HPMW depends on the significant support of intelligence for effectively tracking targets and identification of the radar frequencies and target systems of the enemy. Knowing detailed information about the target allows the employment of a narrow band that ensures the maximum energy delivery to the target to degrade the electrical components (McGonegal, 2020, pp. 3-15). Microwave weapon systems differ from those specific to electronic warfare – limited to jamming – even if both use frequency spectrum against enemy electronics. Microwave weapons – having lasting effects, enemy electronic systems do not have to be in operation, and protection against them involving actions at the system level as a whole – are used to penetrate electronic systems and overwhelm the ability of a target to reject, disperse, or withstand to the energy received (Walling, 2000, p. 2).

HPMS can disable or destroy the electronic equipment used by the adversary. A swarm of drones can be neutralized – degrading the electronic circuitry in drones due to excessive thermal heating, destroying semiconductor junctions or changing memory states in firmware and generating processing errors – by emitting a single short high-power pulse in the gigahertz frequency range. The effectiveness is higher when the pulse's centre frequency coincides with the circuits' resonances. The efficacy is determined by the synchronization of the waveform through which the necessary power for the complete neutralization of each drone in the group is transmitted, at an adequate distance that makes the enemy's operation not have the desired effect (Green, 2022, pp. 1-10). HPMWs, due to the wider effect area, become ideal assets for destroying missions of large drone swarms.

HPM pulses' effects on an electronic device are conditioned by several factors, and can cause ***damage*** or ***upset***. If the electric field magnitude generated by the HPMW pulse has considerable or relatively large dimensions so that it can puncture the oxide layer of semiconductors within the device or causes cascading outcomes on the frequency bands used for data transmission, the result is ***damage***. If the voltages induced in the electronic device are satisfactory or acceptable in quality or quantity to cause a modification of the binary information transmitted or stored in the device or to change the semiconductor switching status within the device, the result is ***upset***. Therefore, according to the physical laws of electromagnetic propagation, the same HPMW pulse could upset electronic devices at a greater range than the distance at which the damage would be caused (Green, pp. 1-10, 71-76).

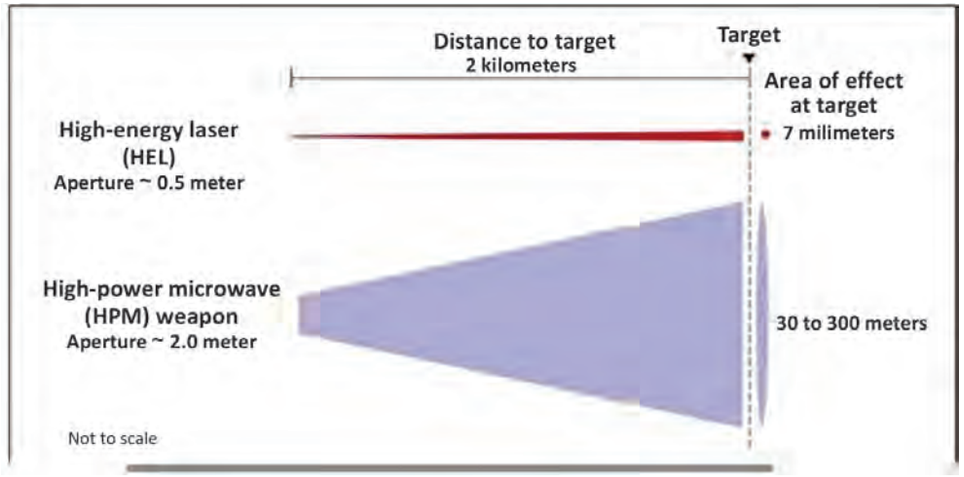


Figure 3: Illustrative effects of HEL weapons compared to HPMW (O'Rourke, 2023, p. 2)

Potential Advantages and Limitations of HPM Weapons

The ***main advantages*** are represented by: *unlimited capacity to execute the fire*; *low cost per shot*; *short time to engage targets* and calibrated responses; *temporary or system-specific effects*. HPM weapons can generate different frequencies and power levels to temporarily or permanently disrupt the electronic systems established as targets without affecting other systems; *extensive effects*. HPM weapons can destroy many unshielded military or commercial electronic systems. Supplementary, they can disable any electronic system located in their electromagnetic cone; *non-lethal applications*. Particular HPM weapons, such as the *"heat rays"*, could represent a non-lethal anti-personal capability in situations in which otherwise the lethal force would have been used; *limited collateral damages*. HPM weapons do not produce collateral damage to physical structures. This feature makes them suitable for actions in urban areas or for punctual situations.

The ***potential limitations*** of the HPM refer to: *constraints about range*. The HPM beams are more diffuse than the lasers and have a lower effect concentration capacity. Therefore, the energy per surface unit decreases in proportion to the distance and the range at which the desired effects can be produced; *fratricide risk*. Because HPM weapons affect all unshielded electronic systems within the range, the own forces systems must be shielded or removed outside the range; and, *the effectiveness of the countermeasures*. The targets shielding favours the absorption of electromagnetic radiation, accordingly, HPM weapons can become ineffective against shielded targets (O'Rourke, 2023, pp. 1-20).

CONCLUSIONS

The conflicts in Ukraine and the Middle East have shown that the threat environment is changing and emerging technologies are increasingly relevant in conflict, modern war, deterrence, and global power balance. The great powers develop programs, in the long and short term, to successfully capitalize on the technologies of the future to identify, research, make prototypes, and subsequently be fielded as operational weapons. Because most joint military actions depend on or are based on the use of electronic devices, the great powers have invested in programs and technologies for the improvement of these assets but also to counteract the operation of these devices.

DEW – unique capabilities – can contribute to coercion by conventional means able to be employed in military operations to change the opponent's behaviour and they can have as target elements that are vital to the enemy state. Due to these possibilities, DEWs represent capable and credible assets that contribute to deterrence and victory in a total war. The DEW – a key element in future wars – can be deployed, by the great powers, in different regions of the globe in situations that are below the threshold of the war, in response to different military actions of some states that represent threats and carry out hostile actions against them. The employment of DEW can lead to communication breakdown in a country by destroying the electrical components, thus limiting the normal working of vital functions in a society and the ability to carry out military actions. DEW can be used for crisis management situations. Currently, many technologies employing directed energy have passed the design-development and manufacturing phase and are in a phase of becoming operational weapons. The procurement of DEWs installed on several different platforms ensures new and innovative ways to neutralize relevant targets and contribute to maintaining the competitive advantage over the adversaries.

DEW represents emergent technology and offers flexibility in making decisions and the possibility of conducting overt or covert actions against adversaries. DEW may represent additional assets to conventional weapons by acting as a viable force multiplier and an option to respond to complex threats. It can be successfully used in disrupting the decision-making centres and communications centres, as well as in disrupting the command-and-control processes. The widespread use of drones in the Ukraine war has led to an equally high demand for anti-drone equipment. DEW is an alternative option, an effective defence asset against armed UAS attacks, widely used in the Russian-Ukrainian war and other regional conflicts. Given that in conflicts drones with low costs and high autonomy are widely employed,

the air defence should be adapted and equipped with highly autonomous non-kinetic assets.

Weapons using directed energy are effective and have been implemented in the operational field, with the potential to be diversified in the next years. DEW represents a disruptive emerging technology that is used and developed by great powers to keep competitive advantage.

An important lesson of the latest conflicts is that achieving success in modern war is also conditioned by the rapid and efficient capitalization on emerging technologies in military operations.

BIBLIOGRAPHY:

1. Booz, A. (May 2024). *Top 10 emerging technologies for DoD and national security*. Velocity Magazine: Special Edition Report, pp. 1-10, 54-60, https://www.boozallen.com/content/dam/home/docs/natsec/top-ten-emerging-technologies.pdf, retrieved on 20 September 2024.
2. Defense Intelligence Agency (2022). *Challenges to Security in Space,* pp. 2-30, 41-48, https://www.dia.mil/Portals/110/Documents/News/Military_Power_Publications/Challenges_Security_Space_2022.pdf, retrieved on 20 September 2024.
3. Demarest, C. (5 January 2023). *China developing own version of JADC2 to counter US,* C4ISRNET, pp. 1-7; *China developing own version of JADC2 to counter US (c4isrnet.com),* retrieved on 20 September 2024.
4. Demarest, C. (23 January 2024). *Directed energy weapons need full Pentagon commitment, industry says.* Defense News, pp. 1-5, defensenews.com, retrieved on 20 September 2024.
5. Demarest, C. (18 September 2023). *Directed energy weapons making jump from sci-fi to real world*, C4ISRNET, pp. 1-12, c4isrnet.com, retrieved on 20 September 2024.
6. Department of Defense (27 October 2022). *The 2022 National Defense Strategy of The United States of America*, U.S. Department of Defense, pp. 1-22, https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF, retrieved on 20 September 2024.
7. Edmund Optics (2023). *Common Laser Types,* Laser Optics Resource Guide, pp. 1-3, *Common Laser Types/Edmund Optics,* retrieved on 20 September 2024.
8. Feickert, A. (12 February 2018). *U.S. Army Weapons-Related Directed Energy (DE) Programs: Background and Potential Issues for Congress.* Congressional Research Service, pp. 1-29, https://crsreports.congress.gov/prod, uct/pdf/R/R45098, retrieved on 20 September 2024.
9. Gertler, J.J. (1987). *Emerging Technologies in the Strategic Arena, A Primer*, Rand Corporation, pp. 1-2, 5-15, retrieved on 20 September 2024.
10. Green, D. (February 2022). *Military Applications of High-Power Microwaves*, Defence Research and Development Canada, pp. 1-10, 71-76, https://cradpdf.drdc-rddc.gc.ca/PDFS/unc427/p816672_A1b.pdf, retrieved on 20 September 2024.
11. Gunzinger, M. (2012). *Changing the game: the promise of directed-energy weapons*. The Center for Strategic and Budgetary Assessments, pp. xiii, 1, 20-28, 36-48,73-103, https://csbaonline.org/uploads/documents/CSBA_ChangingTheGame_ereader.pdf, retrieved on 20 September 2024.

12. *High-energy laser weapons: A defense expert explains how they work and what they are used for* (7 March 2024). The conversation, pp. 1-5, theconversation.com, retrieved on 20 September 2024.
13. Hoehn, J.R. (14 November 2022). *Defense Primer: Military Use of the Electromagnetic Spectrum*, Congressional Research Service, pp. 1-3, https://crsreports.congress.gov/product/pdf/IF/IF11155/15, retrieved on 20 September 2024.
14. Hoehn, J.R. (14 November 2022). *Defense Primer: Electronic Warfare*, Congressional Research Service, pp. 1-3, https://crsreports.congress.gov/product/pdf/IF/IF11118, retrieved on 20 September 2024.
15. Lucas, N.J. (2022). *Defense Primer: U.S. Precision-Guided Munitions*, Congressional Research Service, p. 1, https://crsreports.congress.gov/product/pdf/IF/IF11353, retrieved on 20 September 2024.
16. McGonegal, J. (2020). *High power microwave weapons: disruptive technology for the future,* Air Command and Staff College, spring, pp. 3-15, https://apps.dtic.mil/sti/trecms/pdf/AD1107488.pdf, retrieved on 20 September 2024.
17. North Atlantic Council (10 July 2024). *Washington Summit Declaration issued by the NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Washington, D.C.* pp. 1-6, https://www.nato.int/cps/en/natohq/news_227803.htm, retrieved on 20 September 2024.
18. O'Rourke, R. (22 August 2023). *Department of Defense Directed Energy Weapons: Background and Issues for Congress*, Congressional Research Service, pp. 1-20, https://crsreports.congress.gov/product/pdf/R/R46925/7, retrieved on 20 September 2024.
19. O'Rourke, R. (14 February 2024). *Navy Ship board Lasers: Background and Issues for Congress,* Congressional Research Service, pp. 1-20, https://crsreports.congress.gov/product/pdf/R/R44175/103, retrieved on 20 September 2024.
20. Sayler, K.M. (10 August 2021). *Overview of Department of Defense Use of the Electromagnetic Spectrum*, Congressional Research Service, pp. 1-21, 23-24, https://crsreports.congress.gov/product/pdf/R/R46564, retrieved on 20 September 2024.
21. Sayler, K.M. (2023). *Biometric Technologies and Global Security,* Congressional Research Service, p. 1, https://crsreports.congress.gov/product/pdf/IF/IF11783, retrieved on 20 September 2024.
22. Sayler, K.M. (30 January 2024). *Defense Primer: Emerging Technologies*, Congressional Research Service, pp. 1-3, https://crsreports.congress.gov/product/pdf/IF/IF11105/11, retrieved on 20 September 2024.
23. Sayler, K.M. (1 February 2024). *Defense Primer: Directed-Energy Weapons*, Congressional Research Service, pp. 1-3, https://crsreports.congress.gov/product/pdf/IF/IF11882, retrieved on 20 September 2024.
24. Townshend, A. (February 2019). *Revisiting Deterrence in an Era of Strategic Competition.* Sydney: United States Studies Centre, pp. 2-15, https://cdn.sanity.io/files/ooh1fq7e/production/905518c5dc5275b0875e07640ffb8dc9c6281f0f.pdf/Revisiting-deterrence-in-an-era-of-strategic-competition.pdf, retrieved on 20 September 2024.
25. Walling, E.M. (May 2000). *High Power Microwaves Strategic and Operational Implications for Warfare.* Center for Strategy and Technology Air War College, pp. 2, 11-17, https://apps.dtic.mil/sti/tr/pdf/ADA425472.pdf, retrieved on 20 September 2024.

THE IMPORTANCE OF DEFENCE INTELLIGENCE IN ENSURING AVIATION SECURITY WITHIN THE AIR TRANSPORT SYSTEM

Major (AF) Valentin-Marian IORDACHE

Major (AF) Oana BORDIANU

2nd Lieutenant (AF) Iasmina Georgiana SAUCIUC

90th Airlift Base, Otopeni

DOI: 10.55535/RMT.2024.4.40

Informational support is a fundamental element in decision-making processes. Although the importance and necessity of intelligence has been demonstrated throughout history in armed conflicts, other events with impact on society, such as the terrorist attacks on 11 September 2001, have imposed a change in perception regarding the intelligence support areas of application within the air transport system. Even though aviation safety is the basis of air operations, civil or military, aviation security has become vital due to rapidly and unpredictably changing global security challenges. Nowadays, in the context of global security challenges, lessons learned have led to the involvement of defence information support (intelligence) in ensuring global aviation security; artificial intelligence and advanced technologies enable a quick response to identified threats and risks, an aspect recently demonstrated in the civil air transport system.

Keywords: informational support; aviation security; intelligence; threats; risk;

CONSIDERATIONS REGARDING AIR FORCE INTELLIGENCE

The unique characteristics that differentiate air power from sea or land power generate unique intelligence requirements for supporting air operations. Air power is thus able to respond quickly over long distances and, in various situations, aircraft are the first to reach crisis areas; intelligence support must come in a short time, coherently, from all possible sources so that decision-makers at operational, tactical or strategic level have the necessary information to make decisions in a timely manner. Moreover, air power limitations also generate own intelligence requirements. Transport aircraft and the airports where they operate must be protected; the intelligence product must include assessments of threats nature and capabilities. The number of aircrafts in a country's fleet or organization and their operational costs make them a valuable resource. This aspect, together with the vulnerability to which they are exposed during flight, means that intelligence product must represent an assurance that threats can be avoided or neutralized, when possible. (Keightley, 1996, xi)

Albert Einstein once said: *"The level of intelligence is given by the ability to change".* These words perfectly summarize the challenges of the world we live in, a world marked by rapid technological developments and a constantly evolving security environment. In this context, threats are becoming increasingly diverse and complex, requiring continuous adaptation from all actors involved in maintaining safety, security and stability in air operations (Enache, 2022, p. 73). This principle applies particularly to transport aviation, which ensures both rapid mobility of resources and forces, as well as logistical support in operational environment. Given contemporary threats, the ability to adapt and improve intelligence products in support of air transport operations becomes vital to ensure safety, security and success in the dynamic and unpredictable context of global threats.

For decision-makers, the intelligence product is an essential element in planning and execution of both combat and non-combat operations. It provides assessment of adversary capabilities, vulnerabilities, and intentions, thus empowering decision-makers to prepare and act effectively. Through intelligence products, the centre of gravity of adversaries is identified and their vulnerabilities can be exploited.

The intelligence product, by reducing decision-making uncertainty, mitigates the risk to which own forces are exposed and helps the commander to evaluate the effect of operations. The accuracy and relevance of timely information is the basis for effective planning, being thus essential in the conduct of air operations (Keightley, 1996, xii).

INTELLIGENCE SUPPORT FOR PLANNING AIRLIFT OPERATIONS

Security, safety and efficiency of aeronautical operations in air transport missions are crucial elements for ensuring national and regional security, especially in the current context dominated by uncertainties and complex threats. Intelligence support plays a critical role in maintaining security and efficiency by proactively contributing to their improvement. It entails the collection, analysis and dissemination of essential information that contributes to the prevention of security incidents and to the prompt and effective response to any potential threat. Advanced technologies and artificial intelligence enable real-time monitoring and management of situations, reducing risks and increasing operational efficiency (Chiriac, 2018, p. 6).

Air transport ensures the mobility of resources, people and materials, to the right place and time. Organizing, training and equipping air transport units are elements of a constantly evolving science due to operational results and lessons learned. The doctrine of transport aviation, like any other doctrine, is continuously developed so that the air forces of NATO allies, especially of the United States of America, are able to improve their responsiveness, flexibility and effectiveness in operational areas. The biggest challenges remain when airlift is the only available power projection capability in the operational environment, in hostile areas. In these situations, informational support becomes very important in achieving the objectives. Informational capabilities (intelligence support) are not easy to obtain and require rigorous analysis before applying doctrine principles (Donoho, 1997, p. 4).

In a dynamic and complex global security environment characterized by rapid technological developments and diverse threats, intelligence support has become a crucial element for the success of military airlift missions. Through the effective collection, analysis and dissemination of essential data, intelligence structures contribute to the safe planning and execution of air operations, minimizing risks and maximizing efficiency. Airlift missions, especially those carried out in conflict

zones or high risk environments, require a high level of coordination and security. Through intelligence support, proactive measures can be implemented to ensure mission integrity and minimize associated risks. The mentioned support includes, but is not limited to, threat identification and neutralization, risk assessment, air traffic monitoring and coordination between various agencies and entities involved in air operations.

The role of aviation security is to prevent acts of unlawful interference, essentially by preventing the introduction of dangerous objects such as weapons or explosives into aircraft by passengers or other airport personnel with access to or in the vicinity of the aircraft. The field of aviation security has become a major concern following the terrorist attacks of September 2001. Since that critical moment, the normative framework specific to this field has expanded globally, either at national level or through international cooperation/agreements, or through the International Civil Aviation Organization (ICAO) and Annex 17 to the Chicago Convention, or the universal security control program and other related documents (Debyser, Kuzhym, 2024).

Each element has a well-defined role in air transport operations. These elements are often interdependent. If all requirements are managed properly, then the probability of success of the air transport operations carried out is higher; in the same vein, if the requirements stated above are ignored, then chances are high that successful air transport operations will not be possible. From the planning stage, it must be determined which elements are necessary for success, depending on the context, and which are secondary. Lessons learned from Allied operational experience demonstrate that there are four critical elements to successful airlift operations; if one of these elements is not managed properly, then the entire planned air transport operation cannot be successful. The key elements identified are: *command and control, aircraft availability and capability, support and defensive systems, and intelligence activity*. It is not enough to identify these elements, but they must be applied in a logical sequence in the operational phase (Donoho, 1997, p. 60).

The intelligence product is, logically, the first step; understanding the location, the associated risks and threats affecting safety and security in that region are important as they support decision-making process before allocating necessary resources to conduct air transport operations. Whatever the decision, it is much easier when clear and concise information is available.

The intelligence support process in airlift operations *(figure 1)* can be exemplified as a building. The foundation of the building consists of elements specific to the field of intelligence, which essentially represent the principles of the process; they are the most important element of intelligence support in aviation. Obviously, if other elements are omitted from this process, the whole dynamic and structure affect the accomplishment of objectives. Based on these principles, the key attributes and functions required for the information support process are developed to support the four purposes of airlift operations, namely: *decision support, planning and execution support, operational force support and air operations centre of gravity*. All the elements in *figure 1* must be aligned to the doctrine and be flexible enough in order to be adapted to global threats regardless of challenges so that air operations can be conducted safely and in full security (Keightley, 1996, p. 54).

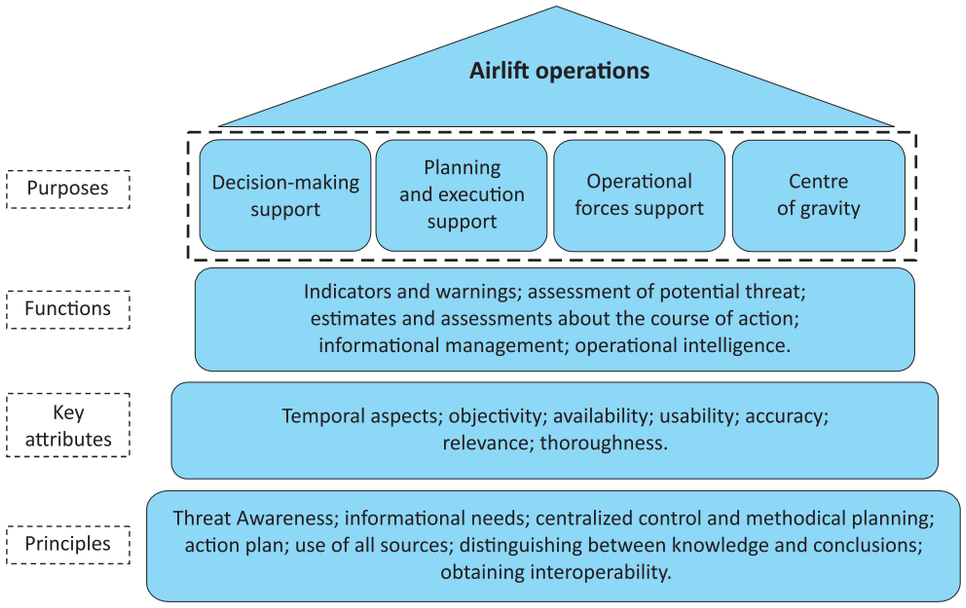


Figure 1: Intelligence support for planning of military or civil air transport operations
(adapted after Keightley, 1996, p. 54)

SUPPORT OF INTELLIGENCE STRUCTURES FOR ENSURING CIVIL AIR SECURITY – EASYJET FLIGHTEZY8303, 3 JULY 2022

In air transport system, security culture entails both compliance with international security standards and promotion of a proactive and responsible attitude towards threat and risk management. In aviation, threats represent the intention to attack a specific target and the probability of this intention to become an actual attack within a specified time frame. In the same vein, risk is the probability that such an attack will be successfully carried out against a target, taking into account the existing vulnerabilities of the respective aeronautical system.

The terrorist attacks on 11 September 2001 represented a dramatic moment in aviation history, demonstrating the impact that terrorism can have on civil aviation, which imposed the development of security management in the air transport system. Those events resulted in significant loss of life, causing significant material and economic damage, and aviation organizations were forced to adopt stricter security measures and invest heavily in technologies and procedures to ensure aviation security

In the face of existing global threats, security management in air transport system requires a multidimensional approach. Reducing vulnerabilities through the development and implementation of clear and rigorous procedures, physical and technological measures, continuous education and training of personnel in the field of crisis management are essential to maintain a safe and secure environment in air transport system.

Developing and promoting a robust security culture is essential for safe and effective air operations to rapidly respond to the dynamic spectrum of global threats. Security culture is not just about complying with regulations, it entails adopting a proactive and responsible mindset among staff and all entities involved to be constantly prepared to manage complex and varied risks.

On 3 July 2022, Aditya Verma, an 18-year-old British man was preparing to board the EasyJet company's Airbus A319 aircraft, flight EZY8303, from Gatwick Airport in England, with five friends, to travel to Menorca, Spain to celebrate the end of school year and the start of holiday. Before boarding the aircraft, Aditya Verma sent a message to his friends on a private group on social networking platform Snapchat in which he wrote: *"I'm going to blow this plane up. I'm a Taliban"*; Aditya Verma later stated that the message was sent as a joke, following the discussions he had with friends regarding who among them would be stopped for a thorough security

check. The 18-year-old British man sent the message from his mobile phone, using mobile data to connect to the internet, and his friends were connected to internet via the Wi-Fi network provided by Gatwick Airport (Gozzi, 2024).

During the flight EasyJet EZY8303, in the airspace of Spain and shortly before the Airbus A319 aircraft began its descent from the assigned flight level to land at Menorca airport, two F-18 Hornet airplanes from the Spanish Air Force military fleet intercepted the civilian aircraft following an order received from national authorities. The captain of Airbus A319 aircraft informed the passengers that he was trying to find out the reasons why the aircraft was intercepted by fighter aircrafts; because of that event, the aircraft landed with a delay of 30 minutes at Menorca airport (Ib.). After landing, the aircraft was parked in an isolated area and, according to the statements from passengers, they waited for approximately four hours on the airport apron as the aircraft was thoroughly checked for explosives by Spanish national authorities.

The EasyJet Airbus aircraft was declared safe and moved next to other commercial aircraft following investigations by specialized teams with dogs specially trained to find explosives. Spanish authorities arrested 18-year-old British Aditya Verma after the aircraft landed; he spent two nights in Menorca prison while the Spanish authorities investigated the incident; he was released on bail. The British intelligence intercepted the message sent by Aditya Verma and it was considered a direct threat to air security. On his return to UK, the British intelligence services, MI-5 and MI-6, interrogated the young man (Hancock, 2024). During the trial that took place at a court in Madrid, Spain, following the incident, the young man stated that *"the intentions was never to cause public distress or cause public harm"*. If found guilty, the British student had to pay the costs incurred by the Spanish Ministry of Defence for alerting and taking off the two F-18 Hornet aircraft that intercepted the Airbus A319 EasyJet aircraft in the amount of 95,000 euros and a fine of 22,500 euros (Gozzi, ib.).

The police said that in the young man's phone they discovered that he had searched the Internet for information about the conflict between India and Pakistan and about the possibility of an attack by the Islamic State in the region, but they did not identify any elements of interest from which it could be concluded that Aditya Verma was radicalized and supported jihad. Asked during the trial what he thought when he saw the aircraft being flanked by fighter jets, Aditya Verma stated that: *"The Russia-Ukraine war was happening so I thought it was a military exercise related to that conflict".* (Hancock, ib.). During the trial not all elements were

clarified; it remained unclear how the message could have been intercepted given that Snapchat app is encrypted, like many other apps available to the general public. One theory, discussed during the trial, was that the message was intercepted via Gatwick Airport's Wi-Fi network, but an airport spokesman said the Wi-Fi network *"does not have that capability".* The judge who presided over the case, quoted by the European press, stated that the message *"for unknown reasons was intercepted by the British intelligence"* (Ib.). In January 2024, the Spanish court acquitted Aditya Verma.

The message sent on the private group by Aditya Verma and intercepted by the British authorities was considered a direct threat to aviation security, the context and content of the message generating an emergency response and swift action from the national security structures. At the same time, the incident demonstrates the vulnerabilities associated with the use of social media platforms; Internet access and the use of electronic devices enable passengers to communicate in real time with family and friends, thus sending messages that can be intercepted and misconstrued inadvertently become real threats to flight security or national security.

British and Spanish authorities reacted immediately after intercepting the message. Treating it as a terrorist threat they activated air security and threat response protocols. At the same time, the event demonstrated the effective cooperation and coordination between national authorities at an international level, in the present case the ones from Great Britain and Spain, regarding aviation security. Fast information sharing and coordination across national security structures are crucial for a prompt response, even if the event exemplified above was not critical, in order to ensure and maintain aviation security.

CONCLUSIONS

Today's aviation security measures, including pre-boarding security screening of passengers, training of airport and aircraft personnel, and advanced technologies used to detect threats, have significantly reduced the chances of a terrorist attack occurring, but have not completely eliminated them. The mentioned incident highlighted the cooperation at the international level between national structures on rapid and effective exchange of information, which demonstrates that there are currently agreements and connections between states to implement common standards and practices and to exchange technologies and information in order to improve global security in commercial aviation field.

However, the incident demonstrates the challenges and vulnerabilities that the technological evolution in aviation security implies. In the future, monitoring systems are likely to become even more sophisticated, integrating emerging technologies such as artificial intelligence to detect unusual behaviour or potential threats. Continuous technological progress and adaptation to global challenges are the basis for effective global aviation security, providing accurate and efficient means to monitor and protect airspace.

Intelligence support is essential to improve air security and efficiency of air transport operations; this support entails collection, analysis and dissemination of relevant information to competent structures and authorities that can prevent aviation security incidents and respond promptly and effectively to any potential threat in the current global context dominated by uncertainties and complex threats.

In conclusion, intelligence support, is an essential pillar in improving aeronautical security in air transport operations. By integrating and implementing advanced technologies, the development of management and information flows, as well as by improving the dissemination process of intelligence products, the effective management of security risks and the safe operation of civil or military transport aircraft are ensured. At the same time, effective informational support contributes decisively to maintaining national and regional security, ensuring that Romania remains a responsible and capable actor in the management of current and future aeronautical and military security crises and challenges.

BIBLIOGRAPHY:

1. Chiriac, C. (2018). *Considerații privind planificarea operațiilor aeriene*. In *Buletinul Universității Naționale de Apărare "Carol I"*. București, https://revista.unap.ro/index.php/revista/article/view/391/366, retrieved on 12 July 2024.
2. Couzens, G., Kraterou, A. (2022). *The Sun: Chess prodigy, 18, who sparked chaos on easyJet flight as he 'threatened to blow up plane' breaks silence after release,* https://www.thesun.co.uk/news/19168510/chess-prodigy-chaos-easyjet-flight-threatened-breaks-silence/, retrieved on 22 August 2024.
3. Debyser, A., Kuzhym, O. (2024). *Transport aerian: Securitatea aviației*, https://www.europarl.europa.eu/factsheets/ro/sheet/132/transportul-aerian-securitatea-aviatiei-civile, retrieved on 22 August 2024.
4. Donoho, J.H (1997). *An Analysis of Tactical Military Airlift. Air Force Institute of Technology*.
5. Enache, P.R. (2022). *Rolul Intelligence în menținerea capacității de luptă în operații militare contemporane*. In *Buletinul Universității Naționale de Apărare "Carol I"*. București, https://revista.unap.ro/index.php/revista/article/view/1389, retrieved on 22 July 2024.
6. Gozzi, L. (2024). *BBC: British man Aditya Verma appears in Spanish court over plane-bomb hoax*, https://www.bbc.com/news/world-europe-68056421, retrieved on 22 August 2024.
7. Hancock, S. (2024). *BBC: British man acquitted over London-Spain flight bomb hoax*, https://www.bbc.com/news/world-europe-68099669, retrieved on 22 August 2024.
8. Keightley, H.B. (1996). *Intelligence Support for Air Operations*. RNZAF.
9. Price, C.P., Forrest, J.S. (2013). *Practical Aviation Security. Predicting and Preventing Future Threats*. Elsevier international. UK.
10. Thomas, A.R. (2008). *Aviation Security Management. The context of aviation security management*. Greenwood Publishing Group. Praeger Security International. USA.

THE EFFECTS OF DEGLOBALIZATION IN THE FORMATION OF A NEW REGIONALIZED WORLD FROM A MILITARY PERSPECTIVE

Colonel Associate Professor George BUCĂŢA, PhD

Lieutenant Colonel Professor Paul TUDORACHE, PhD

"Nicolae Bălcescu" Land Forces Academy, Sibiu, Romania

DOI: 10.55535/RMT.2024.4.41

This article examines the impact of deglobalization on the emergence of a new regionalized world order, with a focus on its military implications. The conflict in Ukraine is highlighted as a pivotal event that underscores the contemporary challenges facing globalization. This conflict accelerates political decisions aimed at navigating a period marked by the erosion of the global order, particularly through dual circulation policies that seek to insulate national economies while leveraging global opportunities. The article discusses how the 2008 financial crisis and subsequent Great Recession weakened globalization both economically and ethically, eroding the credibility of the global financial system. The anticipated resurgence of globalization in the late 2010s failed to materialize, and the 2020s have instead been characterized by disruptions that reveal deep-seated issues within the global system. The article contends that these disruptions are not merely external shocks but symptoms of inherent flaws in globalization, contributing to the formation of a new, more regionalized world order with significant military consequences.

Keywords: deglobalization effect; military deglobalization; regionalized world; military management; global opportunities;

INTRODUCTION

The COVID-19 pandemic had a significant impact on the concept of a *world without boundaries*. In the spring of 2020, numerous nations were compelled to shut down their borders and halt international air travel. Consequently, a large number of expats, who symbolize the phenomenon of globalization, repatriated to their countries of origin. Moreover, the implementation of steps to prevent the spread of contagion resulted in interruptions and deceleration in supply chains, prompting corporations and governments to reevaluate the dangers linked to their worldwide integration. The second distressing incident occurred in February 2022 when Russia invaded Ukraine, further dispelling any last notions of globalization's stability. The implementation of economic penalties on billionaires closely associated with Putin and the removal of Russia from global financial networks, along with the escalating friction between the Western nations and China, serve as additional indications of the demise of globalization as it now stands and as we were acquainted with.

Instead of global integration, it appears that the world is becoming more divided along national and continental lines, with distinct spheres of influence emerging. One such sphere is dominated by China, while another is under the supremacy of the United States of America. This situation is reminiscent of a renewed Cold War. In March 2022, Larry Fink, the director of the financial corporation BlackRock, proclaimed that the conflict in Ukraine signified the culmination of the globalization era that has prevailed for the past three decades. Following the deceleration of global economic integration in the 2000s, we are currently observing a period of genuine deglobalization. This phase of global upheaval is expected to result in a decrease in global interconnectedness, particularly in the medium term. Logistics are being streamlined, firms are implementing re-localization and regionalization strategies for their economic operations, and governments are increasingly interfering in the economic sector, mostly to safeguard it from global disruptions. However, this transformation is not solely attributed to economic developments; rather, it is also influenced by certain political actions. Across several nations, economic policy choices are shifting from a strategy of haphazard worldwide integration to a model of deliberate and regulated integration.

An exemplary illustration may be seen in China, where their 14th five-year plan (2021-25) has prioritized the dual circulation approach, aiming to increase investments in the domestic sector. The objective is to ensure domestic production capability in specific vital industries (such as food, energy, and technology), while allocating greater resources to research and development and infrastructure to maintain competitiveness in the international market. Bidenomics, Joe Biden's economic policy proposal for the White House, was designed with this mindset. The president initiated a plan known as Made in America, with the objective of directing $400 billion annually in US government contracts towards products and services provided by US firms. Within his electoral pledge, he expressed the notion that *"when utilizing taxpayer funds, it is imperative to procure American goods and bolster American employment".* In addition, Biden carefully adhered to Donald Trump's commitment to repatriate manufacturing jobs to the United States of America, pledging to impose penalties on corporations who relocate such employment abroad. Biden's industrial strategy in the strategic electric car industry operates on a same principle, offering substantial tax benefits to incentivize the purchase of domestically built electric vehicles.

The project is a component of a more comprehensive strategy aimed at achieving the objective of *"digital sovereignty"*. This project contradicts the liberalist principle of purchasing products where they are cheapest, but it is justified by prioritizing safety above comfort. Nevertheless, there is widespread scepticism over the presence of the requisite drive for action on the European continent to fully implement a dual circulation strategy. The conflict in Ukraine has compelled Europe to enhance its military and economic alliance with the United States of America, albeit at the expense of compromising certain aspects of its digital sovereignty strategy. It includes reaching a consensus with the USA on transatlantic data flows, which some perceive as a concession to American digital capitalism.

The trend demonstrates that while the integration into the global market was first viewed as a means of achieving economic success throughout the 1990s, it is now also recognized as a potential source of risks. Consequently, there is a growing need to reinstate the regulatory and protective measures implemented by the government. What is required is a more discerning, discriminating, and proactive response to globalization itself. Currently, it appears that China, and to a lesser extent the United States of America, are inclined to adopt this strategy. However, European countries, partly due to their institutional challenges, are still indecisive between the desire to revert to globalization and the recognition of the need to embark on a new course.

The military and security dimensions of this shift toward deglobalization are equally significant. As global interconnectedness diminishes, nations are increasingly prioritizing self-sufficiency and regional alliances, reshaping their defence strategies to address emerging threats in a more fragmented world. The decoupling of global economies has led to the formation of regional blocs with distinct military alliances, similar to the geopolitical alignments seen during the Cold War. The rise of China and the reassertion of Russian influence have intensified military competition, particularly in regions such as the Indo-Pacific and Eastern Europe, where strategic interests are increasingly being defined by regional rather than global considerations.

In this new regionalized world order, military expenditures are expected to rise as countries seek to bolster their defence capabilities in response to the perceived erosion of global security structures. This trend is already evident in the significant increases in defence budgets across NATO countries following the invasion of Ukraine, as well as in the strengthening of regional security agreements like AUKUS (Australia, the United Kingdom, and the United States) in response to China's growing assertiveness.

Furthermore, the shift toward re-localization and the protection of critical industries are also driven by national security concerns. Countries are reassessing their reliance on global supply chains, particularly for essential goods such as semiconductors, pharmaceuticals, and military technologies. The reconfiguration of these supply chains is not just an economic strategy but a critical component of national security, ensuring that key industries remain resilient in the face of global disruptions or geopolitical conflicts.

THE EFFECTS OF DEGLOBALIZATION. NEW REGIONAL POWERS RISING?

The interdependencies formed during the era of extensive globalization have transformed into potent tools: they encompass commercial transactions, the race to construct infrastructure in developing nations, the digital realm with its vast potential to disseminate false information and disinformation, and even migratory movements.

In his 2010 publication titled *"Interdependence Is Truly Intricate"*, Erik Gartzke, a political scientist at the University of San Diego California, presented a thesis that appears self-evident but challenges numerous widely accepted notions about global affairs that have arisen during the era of globalization. Gartzke argues that economic interdependence between countries both promotes peaceful relations and serves as a persistent cause of conflict. The strong connections that bind trade

nations together, fostering their reliance on one another, diminish the occurrence of militarized violence, while simultaneously amplifying clashes of any other kind.

It is not completely contrary to intuition. Nevertheless, within the years of widespread enthusiasm and optimism around globalization and the potential benefits of technology interconnectedness for global unity, this issue was largely overlooked. Politicians, businessmen, and technological experts publicly expressed their belief that the increasing interconnectedness of countries, economies, and cultures could significantly minimize conflicts. This interconnection has not only led to a reduction in wars, but has also aligned the interests of nations in a manner that allows for diplomatic resolution or occasional commercial concessions to resolve any differences. Since 11 September 2001, it has been evident that it is not true. Recently, there have been some unforeseen clashes that have further highlighted this fact. The increased reliance between the European Union and Russia has not alleviated the issues they face. Neither the regions between Central America and North America. Furthermore, there is no relationship between the United States of America and China. The presence of a worldwide discourse on the Internet has not enhanced reciprocal comprehension across nations; instead, it appears that the contrary has occurred.

A similar process of global fragmentation is also taking place within countries. The conflict between diverse groups stemmed from the presence of conflicting interests. However, it is now well recognized that our affiliation with certain organizations plays a significant role in shaping our sense of self and instilling a sense of honour. Unfortunately, it sometimes results in unjustly prejudicing individuals who are affiliated with different groups. Furthermore, we are aware that our discontentment is no longer contingent upon comparison with our neighbours or friends, but it is rather *"universal"* in nature. We always acknowledge that there are always individuals in the world who are, or seem to be, more privileged than us on Instagram. Simultaneously, platforms regulated by algorithms are compelling us to relinquish our ability to make decisions. Governments and corporations are progressively employing algorithms and big data to determine various aspects of our life, including our children's examinations, credit access, job interviews, and healthcare provision. How can the proliferation of anger and conflict be prevented, both within different communities and inside them? (Countering the Cost-of-Living Crisis, WEF, 2022).

The conflict in Ukraine is expected to expedite the path of global transformation. This procedure was already in progress before the epidemic. Discussions had emerged

over novel concepts and notions, such as deglobalization or the waning influence of global value chains. Amidst the pandemic, there has been a surge in the popularity of ideas such as reducing the length of value chains, focusing on local manufacturing, increasing supplier diversity, and retaining larger stock levels. Additionally, there has been a shift towards adopting just-in-case supply methods instead of relying only on just-in-time approaches. Over the course of time, and so forth. The conflict in Ukraine is exerting a significant immediate influence on global economic interactions. The war mostly impacts the enterprises operating in Ukraine and Russia. It has caused interruptions in the flow of goods and services. The impact on the availability of agricultural items and other resources from Ukraine and Russia is of significant evidence. It would intensify inflationary pressures and perhaps result in demonstrations and social unrest in underdeveloped nations. Disruptions in food markets have a strong association with societal instability.

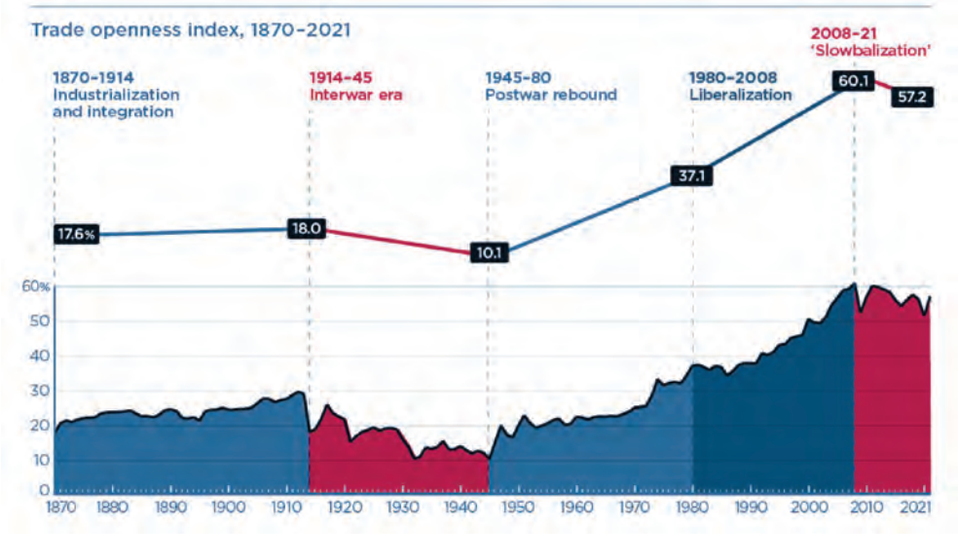


Figure 1: Globalization is in retreat for the first time since the Second World War
(Peterson Institute of International Economics, 2022)

However, the primary purpose of this essay is not to examine the immediate effects of war, which are very unclear and depend mostly on the duration and extent of the military battle. One immediate outcome is that geopolitical risk will significantly increase in importance, particularly for governments and enterprises. The previously unimaginable scenario of a war in Europe has already materialized due to Russia's aggressive invasion of Ukraine. Trust, a crucial determinant

in the conduct of economic actors, will be compromised, hence adversely affecting investments and the overall performance of economic agents. The battle will solidify the formation of two major alliances: a democratic-Western alliance and an authoritarian alliance centred around the Moscow-Beijing axis. China's failure to denounce the invasion of Ukraine might be interpreted as tacit endorsement of the action. Furthermore, it extensively endorses Russia's propaganda and misinformation activities.

The conflict will amplify the alterations in the previously indicated global value chains: reducing their length, promoting regionalization, and fostering the diversification of suppliers, among other effects. Furthermore, there will be significant alterations in the sectorial composition of economies, with increased investments in defence, renewable energy, cyber security, transportation, and logistics. However, warfare may also exert a significant impact on the geographical aspects of global economic ties. In the future, democratic nations may give higher importance to their relationships with countries that share similar values, adhere to conventions, and uphold commitments.

The emerging conflicts involve additional participants such as paramilitary factions, self-defence militias, foreign mercenaries, criminal organizations, and terrorist organizations. These players deviate from traditional guerrilla groups from the 1970s and lack distinct ideological or political affiliations. Most violent groups lack a distinct ethical or political philosophy and do not advocate for Human Rights or Democracy. Generally speaking, these groups employ violence as a means of survival or to acquire positions of power and riches. Irregular soldiers are enlisted through street recruitment, targeting urban gangs and jails. They undergo training in covert camps and are provided with weaponry, generally sourced from the state. Essentially, irregular soldiers are formed to execute acts of ethnic cleansing or massacres that the state is hesitant to perform openly, allowing it to formally disclaim responsibility for such atrocities. The war has been transformed into a franchise that is delegated to private corporations in order to evade the moral accountability linked to professional military men. Essentially, the new wars may be described as the creation of a war model that enables the state to evade the obligations imposed on it by international accords, such as the Geneva Conventions, and a model of a ruthless combatant or warrior.

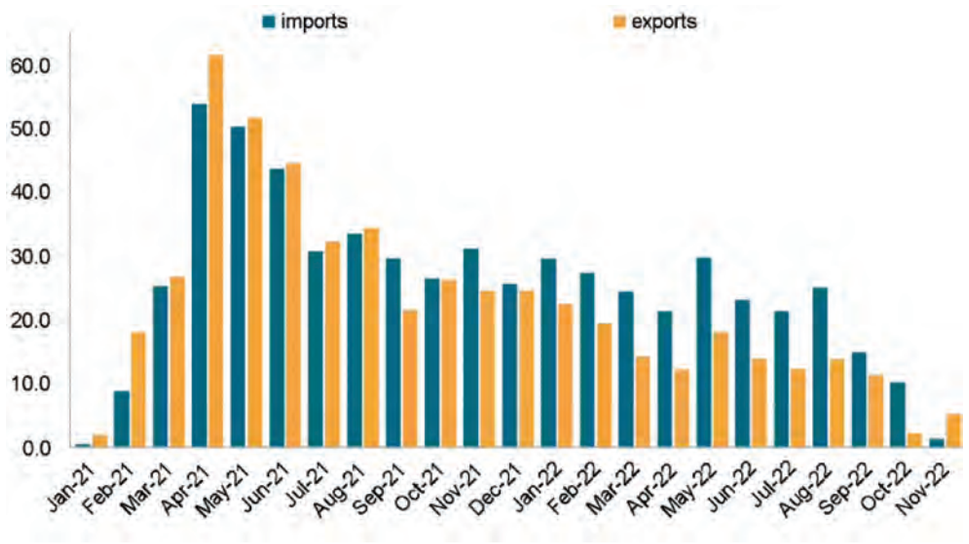


Figure 2: Average year-on-year growth rates for top 10 economies of exports and imports, a sign of deglobalization (SAP Global Market Intelligence, 2023)

The geopolitical landscape has grown increasingly unstable due to escalating hostilities between states, resulting in heightened geopolitical risks that pose a danger to global trade. Both the United States of America and China have implemented trade restrictions and tariffs on each other's goods. Although there is a stated intention to engage in further discussions and strive for a more extensive trade agreement, several tariffs are nevertheless enforced by both parties. Despite the USA and China reaching an agreement to cooperate on global matters such as climate change and trade, the bilateral relationship between the two countries remains intricate. The future development of that connection will have significant implications for the trend towards deglobalization. The presence of unresolved trade concerns generates an atmosphere of uncertainty and instability, which is unfavourable for global markets.

The incursion of Russia into Ukraine in 2022 caused significant upheaval in the economic stability of Eastern Europe, resulting in disruptions to the region's commerce, economy, and energy distribution. Consequently, there has been a renewed emphasis on ensuring energy security and a possible shift away from globalization as nations turn their attention home to prioritize internal resilience above international trade. The geopolitical dynamics of the oil market have grown increasingly controversial, as government actions in Beijing, Brussels, Moscow, Riyadh, and Washington, DC, exert influence over oil prices and the movement

of oil. Both the United States and the European Union have implemented stringent sanctions against Russia's energy sector. Meanwhile, the relaxation of COVID-19 limits in China will significantly influence the future rise in oil consumption. The sanctions placed on Russia by the European Union, United States, and their allies have significant ramifications for the worldwide energy industry.

The G-7 nations have implemented economic sanctions on Russia, while the European Union has implemented price limitations on Russian natural gas. Consequently, there is now a constrained energy market in the short term. Consequently, petrol prices in Europe have risen, and it is anticipated that they will stay at a high level during the winter of 2023-2024, before subsequently decreasing. In addition, it is forecasted that global oil prices would increase to $110 per barrel over the period of 2023-2024, and thereafter decrease to an average of $85 per barrel in 2025. The invasion of Ukraine by Russia has compelled non-European nations to address global threats such as the spread of nuclear weapons, cyber-attacks, the ability of infrastructure to withstand disruptions, and the viability of security alliances in the future (Xing, Bernal-Meza, 2022).

The future will be characterized by a series of common obstacles – climate vulnerability, facilitating the shift to renewable energy, transformative technology and safeguarding against cyber threats, social disparities, and global health crises. However, the ongoing expansion of international commerce has prompted concerns among nations and corporations, particularly over the vulnerabilities associated with dependency. The concept of globalization, which involves the interconnection of nations and companies through macroeconomic factors, trade regulations, and global supply chains, is currently being reevaluated owing to concerns related to policy, security, and economic matters. Consequently, several governments, businesses, and civil actors are contemplating the benefits of adopting a more self-contained approach to trade and commerce, as countries strive to establish their position in a swiftly evolving environment. This move, sometimes referred to as *"deglobalization",* poses an emerging geopolitical danger for firms.

The 2008 global financial crisis played a major role in fuelling the deglobalization movement. As a reaction to the worldwide economic instability, several governments shifted their policies and communication towards protectionism, implementing restrictions on the unrestricted movement of trade and investment between countries. In recent times, the worldwide pandemic and Russia's invasion of Ukraine have contributed to the rise of protectionist measures. After the invasion, the International Food Policy Research Institute reported that 24 nations enforced export restrictions on essential food items including wheat, sugar, and oils.

The combination of sudden disruptions in the supply chain and increasing protectionist measures has generated concerns about potential shortages. As a result, governments are contemplating various strategies, including reshoring (bringing their supply chains back to their own country), near shoring (establishing supply chains with neighbouring countries), and friend shoring (relying on trusted allies for their supply chains). In response to current geopolitical changes, governments are actively implementing industrial strategies. The US CHIPS and Science Act, enacted in 2022, and the European Chips Act, endorsed in April, were both prompted by the worldwide semiconductor shortage. Their objective is to guarantee sufficient production of domestically manufactured chips in the US and the EU, even if it means incurring higher costs compared to imported alternatives (Ozili, 2022).

The presence of complex social issues has played a role in the discussion around globalization and its impacts. The advent of interrelated hazards at the national level has compelled enterprises to reassess their operations in a post-pandemic age. The hazards encompass climatic risk, economic and inflationary factors, international security concerns, COVID-19 recovery endeavours, trade flows, and credit accessibility. Although the discussion on deglobalization is expected to continue, S&P Global Market Intelligence's extensive trade data suggests that global commerce will likely resume a long-term pattern of growth in the coming years. Currently, deglobalization is primarily a matter of rhetoric rather than an actual economic movement. Nevertheless, the dangers associated with deglobalization are genuine and significant.

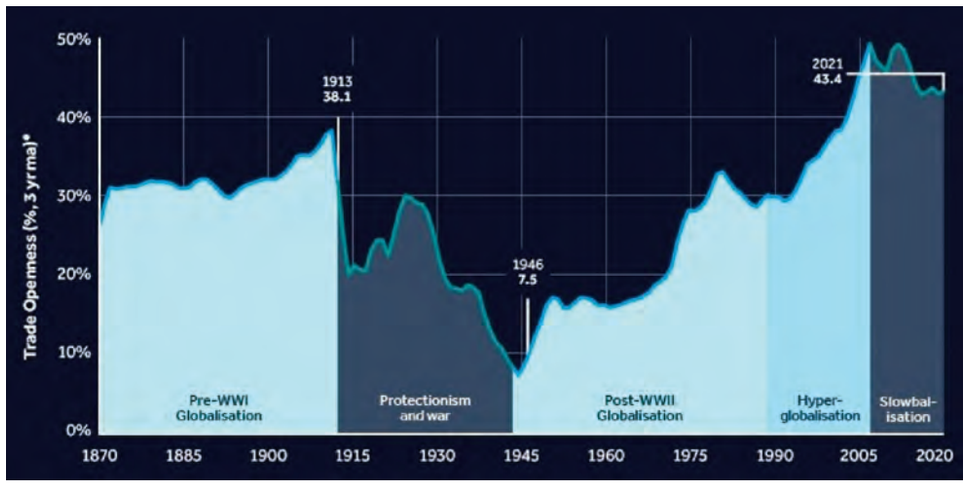


Figure 3: Globalization through recent history (World Economic Forum, 2023)

On the occasion of the prolonged Yugoslav conflicts and the events on 11 September 2001, an important group of international analysts began to take an interest in the various forms that wars take in conditions of intense globalization. In order to understand the particularities of this type of phenomenon in the post-Cold War world, most of these analysts have undertaken a comparative exercise with previous forms of war, and the dissimilarities that current wars register with respect to past ones. They infer the points of convergence that arise between these modalities of conflict and globalization.

From such an argumentative perspective, these scholars emphasize that from the emergence of the modern state in Europe until the end of the 20th century, wars played a central role in the life of nations. They repeatedly refer to Michael Mann's monumental work, *The Sources of Social Power*, to demonstrate that until well into the 20th century, more than half of the state's resources were allocated to military functions, with military performance being one of the main stimuli to increase state finances and develop the national space. In this important role that corresponded to military power, different elements influenced, such as the ambitions of the rulers, internal considerations as well as the very dynamics assumed by the international system, since *"individual states, to guarantee their own security, had to prepare for war, a process that was enough to generate insecurity in the other states and led them to respond in kind. In short, states armed and militarized themselves in part to increase their own security and, in doing so, increased the insecurity of other states, which in turn resorted to weaponization"* (Lo, Marcelin, Bassène, Sène, 2022).

During this process of consolidation and strengthening of states, several types of wars were witnessed: the first, predominant in the 17th and 18th centuries, were spatially limited, although sometimes of very long duration, and responded to the need to establish power by the absolutist states; then a new stage appeared that covered almost the entire 19th century, which was characterized by the fact that wars assumed a national and revolutionary format and were fundamentally centred around the problem of the creation of nation-states; next, we entered an era of total wars at the beginning of the 20th century (First and Second World Wars), with a high ideological, nationalist and political content, and finally, the world had to face the *"imaginary"* Cold War, based on nuclear deterrence, crystallized around certain political and ideological references that gave it support and coherence. All these types of war, even though they obeyed different war modalities, given that they were singular in terms of their objectives, dissimilar in the types of armed forces they used, in military technique and in the war economy, shared certain common

features: they were forms of violence organized by states or by political groups conceived for political reasons; those who resorted to war intended to exercise control over certain territorial spaces, establishing a more or less spontaneous distinction between the internal and the external, the public and the private; they reproduced a roughly clear differentiation between war, on the one hand, and other types of conflict and violence, on the other hand; the state acted as an *"organizing"* agent of the war, the armed forces, even when they were civil wars, were organized hierarchically and the war economy was structured from a state and *"national"* point of view (Shelest, 2015).

The onset of the pandemic resulted in the shutdown of the worldwide economy and alterations in overall consumer preferences, which were the prominent topics until the Russian invasion of Ukraine in February 2022. The constraints, resulting from the combined impact of shifts in spending patterns and reduced activity in the business sector, precipitated a worldwide economic crisis and led to a sharp increase in inflation. Over that period, there was a lack of toy deliveries over Christmas, which prompted governments to quickly recognize more significant weaknesses that posed a threat to the strategic independence of their nations. The disintegration of the value chains of microchips and other vital industrial materials caused significant concern.

Several months later, the Russian incursion into Ukraine once again impacted the oil industry, particularly in terms of its significant geopolitical implications. The few diplomatic relations that persisted between the European Union and Russia have been completely broken, and we are currently witnessing yet another conflict in Europe, which is causing great distress. The German response to the rise in military expenditure and the delivery of weapons to Ukraine, if grudgingly, signifies a complete reversal in its foreign policy and indicates a broader inclination towards military buildup and alignment of international objectives within the so-called *"Western world"*. The energy diversification plans for 2025 and the ongoing activities, such as the importation of liquefied gas and the reassessment of the Maghreb, are indicative of strategic deglobalization. Therefore, we foresee a fragmented kind of globalization that is limited to geopolitical blocs, ensuring the security of their respective supply chains. It appears that we are gradually moving towards that future.

Some individuals contend that deglobalization is a consequence of these disturbances. Undoubtedly, the epidemic has caused a decline in international trade, and it is anticipated that more disruptions will occur as a result of the Russian

invasion and the accompanying sanctions. However, strategic deglobalization extends beyond these factors. This process predates the epidemic and originates from the liberal international order's inability to retain its dominant position, both internally and externally, and effectively communicate its worldview to the global community. Following the experiences in Iraq and Afghanistan, the previously held belief in the inherent positivity of the system is now seen as simplistic and is rapidly being replaced by an acknowledgment of the constraints of liberal democracies and the unpredictable nature of International Relations (Rodrik, 2021).

First and foremost, the liberal international order has experienced internal attacks. While political liberalism still exists, it faces growing scrutiny from illiberal forces that are spreading worldwide. These movements prioritize material concerns and the widening wealth disparities within nations, which are linked to the decline of middle-class aspirations. Simultaneously, the system is also being questioned from external sources. The dominance of the United States of America, albeit present in many domains, is being supplanted by a more diverse and multipolar global order. Nevertheless, the capability of multilateral organizations, such as the United Nations (UN), the World Trade Organization (WTO), or the International Monetary Fund (IMF), to influence the worldwide agenda has been diminishing, along with their ability to make decisive decisions. The tepid denunciation of the Russian incursion at the General Assembly serves as compelling evidence of it (Bharti, 2022).

The significant transformations in recent years challenge the certainties that we previously held, which were based on limited possibilities. It places the researcher in a position of both accountability and unpredictability. Models, which are fundamental frameworks for interpreting data, are utilized until they become obsolete and necessitate replacement. This essay contends that strategic deglobalization is currently the prevailing phenomenon in the international system, and its effects on the geoeconomic and geostrategic domains are already evident. The responses to the epidemic and the Russian incursion serve as both catalysts and integral components of this phenomenon. From this standpoint, partial deglobalization appears to be the most likely outcome of the transition towards a multipolar system.

The Ukrainian war-induced fuel and food shortages are worsening the already elevated post-pandemic inflation, which had already reached its worst levels in decades throughout much of the world, therefore impacting the global economy. It would be an exaggeration to claim that the causes are fully understood, as academic

macroeconomists are still perplexed by the ultralow inflation of the 2010s. But the primary factors are evident. Initially, governments and central banks were sluggish in reversing the extraordinary macroeconomic boost implemented during a period of calm. Undoubtedly, the initial stimulus measures provided significant support during the early phase of the epidemic. However, in many instances, these measures remained in place for an extended period and became excessive following the surprisingly rapid recovery in advanced countries and certain emerging markets. In the United States of America, specifically, the confluence of a $900 billion fiscal stimulus at the end of 2020, coupled with a subsequent $1.7 trillion package in March 2021, proved to be excessive and untimely.

Supply chain interruptions have significantly contributed to inflation, while a portion of the supply pressure can be attributed to the abrupt increase in demand. In sophisticated countries, notably the United States of America and the euro area, over 50% experienced inflation rates above 5% even prior to the outbreak of hostilities. Consequently, the conflict exacerbated an already challenging position. Before the conflict, the combined wheat exports of Russia and Ukraine were 25% of the world total. Additionally, Russia had a significant role as a supplier of fossil fuels, particularly to Europe. The increase in pricing is being caused by disruptions to the supply of certain goods (Brancaccio, De Cristofaro, 2022).

MILITARY IMPLICATIONS OF DEGLOBALIZATION IN A FRAGMENTED WORLD

The ongoing process of deglobalization is profoundly changing the global order, with significant implications for military strategy, regional security and the formation of new alliances. As the world retreats from the extensive interconnectedness that characterized the late 20th and early 21st centuries, nations are increasingly focusing on regional stability, self-sufficiency and the recalibration of military alliances. This shift is particularly evident in regions bordering active conflict zones and among major military powers seeking to assert their influence in a more fragmented world.

The most immediate and tangible military effects of deglobalization can be observed in countries bordering conflict zones such as Ukraine. The Russian invasion of Ukraine in 2022 not only destabilized Eastern Europe, but also triggered a significant reassessment of military positions across the continent. For countries such as Poland, Romania and the Baltic states, the threat of further Russian aggression has led to an urgent need to strengthen their defence capabilities. These countries have increased their military spending, modernized their armed

forces and sought closer security ties with NATO and the European Union. The presence of NATO forces in Eastern Europe has been significantly strengthened through new deployments and the establishment of permanent bases to prevent further Russian advances.

In addition to traditional military measures, these countries are also investing in asymmetric warfare capabilities, such as cyber defence and information warfare, to counter the multi-layered nature of modern conflicts. The war in Ukraine has shown how important cyber operations, both offensive and defensive, are in modern warfare. Neighbouring states have taken note and realized that the battlefield is no longer limited to physical territory, but also extends to the digital realm. This realization has led to a broader reassessment of what constitutes national security, with the protection of critical infrastructure and countering disinformation campaigns becoming increasingly important.

The impact of the conflict in Ukraine is increasingly being felt in other regions, particularly in the Indo-Pacific region, where the strategic calculus of major powers such as the United States of America, China and India is being redefined. Rising tensions between China and its neighbours such as Japan and Australia have accelerated the formation of new military alliances and the strengthening of existing ones. The AUKUS pact, which includes Australia, the United Kingdom and the United States, is a direct response to China's growing assertiveness in the South China Sea and the wider Indo-Pacific region. This alliance, which includes plans for Australia to acquire nuclear-powered submarines, represents a significant shift in the regional balance of power and underlines the importance of military partnerships in an era of deglobalization. Secretary of Defense Lloyd J. Austin III Statement on Two-Year Anniversary of AUKUS mentioned that: *"I am incredibly proud of the tireless work of this department and our U.K. and Australian counterparts, and I am confident in the bright future of our historic partnership. Working together over these past two years, we have accelerated efforts toward our common goals faster than anyone would have thought possible".*

The United States of America has recognized the changing dynamics of global power and is also seeking to deepen its military relationship with India, a major player in the Indo-Pacific region. The US-India defence relationship has grown significantly in recent years, reflected in increased joint exercises, arms sales and intelligence sharing. This partnership is part of a broader strategy aimed at counterbalancing China's influence in the region and securing critical sea lanes essential to global trade. As deglobalization progresses, such regional

alliances are likely to become more important as localized security arrangements are needed in a world where global institutions are losing their effectiveness. The latest data from the Stockholm International Peace Research Institute (SIPRI) on global military spending shows that for the first time in 2021, the world spent more than 2 trillion US dollars on the military. It set a new record after seven consecutive years of increases *(figure 4).*

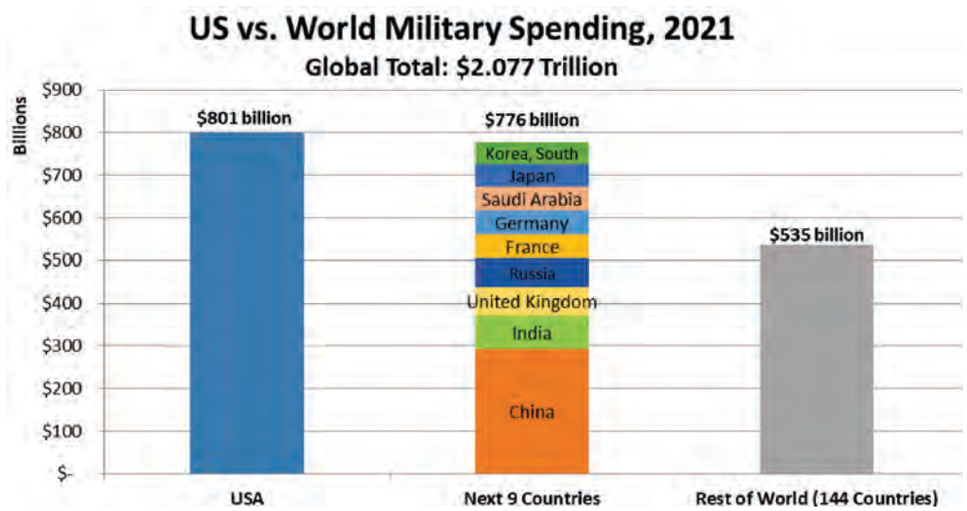


Figure 4: Situation of global military spending
(https://www.nationalpriorities.org/blog/2022/06/22/us-still-spends-more-military-next-nine-countries-combined/)

At the same time, deglobalization is leading to the emergence of new, less formalized alliances driven by common interests and mutual concerns rather than traditional treaty obligations. These coalitions often emerge in response to specific threats or regional instability and may include a mix of state and non-state actors. In the Middle East, for example, the shifting loyalties and complex interplay of regional powers have led to ad hoc military collaborations, such as the Saudi Arabia-led coalition in Yemen. These alliances tend to be fluid and opportunistic, reflecting the fragmented nature of the current global order.

The decline of globalization also has significant implications for the arms trade and military technology. As countries become more inward-looking and prioritize national security over global cooperation, there is a growing trend toward the indigenization of defence industries. Nations are increasingly seeking to reduce their dependence on foreign arms suppliers by developing their own military

technologies. This shift is particularly evident in countries like India and Türkiye, which have embarked on ambitious programs to build domestic defence capabilities. The emphasis on self-sufficiency in defence production not only reduces vulnerability to external pressures but also strengthens national security by ensuring that critical military supplies are not subject to international sanctions or supply chain disruptions.

The strategic decoupling between the West and countries such as China and Russia represents one of the most significant shifts in the global military landscape in recent decades. This decoupling is not only a geopolitical or economic phenomenon, but also a decisive factor in the development of military technology and capabilities. As the West, particularly the United States of America and its allies, increasingly impose export controls, sanctions and other restrictions on the transfer of advanced technologies to China and Russia, these countries are forced to accelerate their efforts to develop indigenous alternatives. This process is leading to a bifurcation of global military technology standards with profound and potentially destabilizing implications.

The technological divide is evident in several key areas, including missile defence systems, cyber capabilities, artificial intelligence (AI) and advanced weapons platforms. For example, while the West continues to invest heavily in network-centric warfare systems that rely on seamless communication and data sharing between different platforms, China and Russia are developing their own systems that may not be compatible with Western technologies. This divergence is leading to the emergence of parallel military technology ecosystems, each with their own standards, protocols and operational doctrines.

In the area of missile defence, for example, the USA and its allies have focused on systems such as the Aegis Ballistic Missile Defense System and the Terminal High Altitude Area Defense (THAAD). Meanwhile, Russia has developed its S-400 and S-500 systems, which are being sold to various countries, including India and Türkiye. China is also continuing to develop its own missile defence capabilities with systems such as the HQ-9. The presence of these disparate systems complicates efforts at military cooperation and interoperability, especially between nations that may be allied with both Western and non-Western powers.

The lack of interoperability between these disparate systems poses a major challenge to coalition warfare, where the ability of different nations' militaries to work together seamlessly is critical. In a conflict involving both Western and non-Western allies, the technological incompatibilities could lead to operational

inefficiencies, communication breakdowns and reduced combat power. For example, if a NATO member is operating alongside a non-NATO ally that has Russian or Chinese systems, the two forces may have difficulty coordinating their actions, sharing intelligence or integrating their missile defence capabilities, which could jeopardize the success of joint operations.

Furthermore, this bifurcation could lead to a fragmentation of global military alliances, as countries may be forced to choose between aligning with Western or non-Western military technologies. Nations that have traditionally taken a neutral stance or sought balanced relations with both blocs may find it increasingly difficult to do so, leading to a more polarized international system. This polarization could in turn exacerbate tensions and increase the likelihood of regional conflicts as countries align themselves with one or the other technological standard, which could lead to proxy wars or arms races in different parts of the world.

The technological divide is also driving innovation in asymmetric capabilities. As China and Russia seek to counterbalance the West's traditional military superiority, they are focusing on areas where they can gain an advantage, such as hypersonic weapons, anti-satellite systems (ASAT) and cyber warfare. Hypersonic weapons, which can travel at speeds in excess of Mach 5 and manoeuvre to avoid detection and interception, are of key importance to both China and Russia. These weapons could render existing missile defence systems obsolete and shift the balance of power in their favour.

In the space domain, both countries are developing ASAT capabilities to attack the satellites that form the backbone of Western military communications, navigation and surveillance systems. The ability to jam or destroy these satellites could cripple the West's ability to conduct military operations, especially those that rely on precision-guided munitions and real-time reconnaissance. Meanwhile, in cyberspace, China and Russia are investing heavily in offensive cyber capabilities to penetrate and disrupt Western networks, further complicating their adversaries' defence strategies.

The long-term strategic implications of this technological bifurcation are profound. As the West, China, and Russia continue to diverge in their military technologies and doctrines, the risk of miscalculations and misunderstandings in a conflict scenario increases. Each side's reliance on its own systems, coupled with a potential lack of transparency or mutual understanding of capabilities, could lead to escalation in a crisis situation. For instance, the deployment of new, untested technologies in a tense geopolitical environment could be misinterpreted

as an aggressive move, prompting a disproportionate response and potentially leading to a broader conflict.

We can expect that bifurcation of military technology standards could hamper global efforts to control the proliferation of advanced weapons. As China and Russia export their systems to countries outside the Western sphere, the spread of incompatible technologies could complicate arms control agreements and non-proliferation efforts. Multiple and competing technological standards could also make it more difficult to establish global rules and regulations governing the use of emerging technologies such as artificial intelligence and autonomous weapon systems.

CONCLUSIONS

The military implications of deglobalization are profound and multifaceted. As the world becomes more regionalized and less interconnected, nations are reassessing their security strategies, forming new alliances, and investing in self-sufficiency. The fragmentation of the global order is leading to a more unpredictable and potentially volatile international environment, where regional powers play a more prominent role, and traditional alliances are supplemented by more fluid and issue-based coalitions. In this new era, military power is increasingly defined by the ability to adapt to a rapidly changing geopolitical landscape, where the old certainties of globalization no longer apply. The bifurcation of military technology standards has far-reaching implications for coalition warfare, global security, and the future of international alliances. As the world moves further into this era of technological divergence, the risks of conflict and instability are likely to increase, making it more important than ever for nations to find ways to manage their differences and cooperate on critical security issues.

The risks associated with deglobalization have significantly increased since the invasion of Ukraine. Following the onset of the pandemic, there was significant discourse surrounding the enhancement of supply chains' resilience and reducing dependence on imports for critical public health supplies like vaccines, antibiotics, and essential components like semiconductors that underpin the digital economy. The abandonment of Asia's *zero-COVID* policy is leading to a rise in supply disruptions, offering a preview of the potential effects of transitory deglobalization. Undoubtedly, Russia is poised to experience prolonged isolation. However, the true impact on globalization will occur if trade between developed nations and China also declines, which regrettably remains a possibility in certain situations.

The geopolitical stability is unlikely to benefit from a significant reconfiguration of the global economy. Political economists have contended, following Montesquieu, that nations engaged in commerce are less prone to engage in warfare. A contemporary refinement of this notion is that even indirect trade facilitated by shared partners and networks contributes to this effect.

Crucially, these approximate estimations are contingent upon several assumptions, such as the extent to which nations may readily replace imported commodities with domestic alternatives or engage in trade with alternative partners. Furthermore, if trade deglobalization results in increased markups by local monopolistic suppliers and reduced *"creative destruction"* in the economy, the associated costs might be considerably elevated. Globalization can have dynamic impacts that are not included by present models, in addition to beneficial benefits on a country's institutional development. Moreover, similar to how there might be significant losers from globalization, despite the substantial gains of the winners, the consequences of deglobalization are expected to disproportionately impact certain industries, hence magnifying the overall impacts.

The process of globalization has begun to stabilize since its peak before the global financial crisis. However, although it is probable that the Russia-Ukraine war would cause a shift in the Russian economy away from the Western countries, we are cautious about forecasting wider tendencies of deglobalization arising from this conflict. Specifically, claims regarding the potential loss of the dollar's role as a reserve currency or the emergence of a significant *"Eurasian"* global trade axis appear to be overstated.

It is premature to discuss substantial deglobalization at this point. Instead, there has been a stabilization of the proportion of global commerce in relation to GDP and some indicators of financial globalization. This current situation does not closely resemble other eras of deglobalization, such as the interwar years. Russia is undoubtedly seeing a significant shift in its economic and financial connections. Nevertheless, the limited scale of its economy means that it will have minimal direct influence on wider globalization patterns. Furthermore, the formation of a prospective *"Eurasian"* trading bloc is unlikely to fragment global commerce.

In 2020, the combined bilateral commerce among China, Russia, and India was a mere US$200 billion, which falls short of the total imports of nations such as Thailand or Türkiye. Even if that were to increase double or thrice, it would still be a small fraction of global commerce. Furthermore, China's commerce is predominantly focused on the United States of America and its allies. The worldwide currency status

of the dollar is unlikely to face any significant challenges. Economies contemplating a transition from the dollar face a dearth of viable alternatives, since the dollar's supremacy is firmly established due to the extensive US financial markets and its predominant role in global trade invoicing. China's Yuan has limited worldwide currency usage and has seen no significant growth according to some indicators. The potential conversion of certain oil trade flows into alternate currencies does not constitute a significant threat to the stability of the dollar. The oil trade accounts for just 10% of the total value of commerce conducted in US dollars worldwide. Even if a small amount of Saudi Arabia's crude oil shipments to China were to be priced in a different currency, it would not significantly impact the overall demand for US dollars on a global scale.

BIBLIOGRAPHICAL REFERENCES:

1. Aiyar, S., Chen, J., Ebeke, C. H., Garcia-Saltos, R., Gudmundsson, T.&Ilyina, A., Kangur, A., Kunaratskul, T., Rodriguez, S.L., Ruta, M., Schulze, T., Soderberg, G., Trevino, J.P. (2023). *Geoeconomic fragmentation and the future of multilateralism*. New York: International Monetary Fund, 2023.
2. Brancaccio, E., Cristofaro, F, de (2022). *In praise of 'general laws' of capitalism: notes from a debate with Daron Acemoglu*. In *Review of Political Economy,* pp. 1-15. doi: https://doi.org/10.1080/09538259.2022.2037930, https://doi.org/10.1080/09538259.2022.2037930, retrieved on 22 July 2024.
3. Bharti, S.S. (2022). *The re-emergence of the Ukraine crisis and role of the European Union in the de-escalation of conflicts.* European Journal of Transformation Studies, 10(1), pp. 6-19.
4. *Deglobalisation: what you need to know* (January 2023). World Economic Forum, https://www.weforum.org/agenda/2023/01/deglobalisation-what-you-need-to-know-wef23/, retrieved on 23 January 2024.
5. Gartzke, E. (15 February 2010). *Interdependence Really is Complex*, https://pages.ucsd.edu/~egartzke/papers/complexinterdep_02242010.pdf, retrieved on 29 June 2024.
6. *Globalization retreat first time after second world war*, https://www.piie.com/research/piie-charts/globalization-retreat-first-time-second-world-war, retrieved on 22 July 2024.
7. IMF (October 2022). World Economic Outlook: Countering the Cost-of-Living Crisis, https://www.imf.org/en/Publications/WEO/Issues/2022/10/11/world-economic-outlook-october-2022, retrieved on 22 January 2024.
8. Lo, G.D., Marcelin, I., Bassène, T., Sène, B. (2022). *The Russo-Ukrainian war and financial markets: the role of dependence on Russian commodities*. Finance Research Letters, 50, 103194.
9. Ozili, P.K (2022). *COVID-19 in Africa: socio-economic impact, policy response and opportunities. International Journal of Sociology and Social Policy*, 42(3/4), pp. 177-200.

10. Peksen, D. (2019). *When do imposed economic sanctions work? A critical review of the sanctions effectiveness literature*. Defence and Peace Economics 30, no. 6 (2019), pp. 635-647. doi, https://doi.org/10.1080/10242694.2019.1625250, retrieved on 22 July 2024.
11. Rodrik, D. *Why does globalization fuel populism? Economics, culture, and the rise of right-wing populism.* Annu Rev Econ. 2021; 13:133–170. doi: 10.1146/annurev-economics-070220-032416, retrieved on 12 July 2024.
12. Shelest, H. (2015). *After the Ukrainian crisis: Is there a place for Russia?* Southeast European and Black Sea Studies, 15(2), pp. 191-201.
13. Xing, L., Bernal-Meza, R. (2022). *China-US rivalry: a new Cold War or capitalism's intra-core competition?* In Brasileira de Política Internacional 64, no. 1, pp. 1-20. doi: https://doi.org/10.1590/0034-7329202100110, retrieved on 22 July 2024.
14. https://www.nationalpriorities.org/blog/2022/06/22/us-still-spends-more-military-next-nine-countries-combined/, retrieved on 22 July 2024.

PUBLIC DIPLOMACY IN THE ERA OF ARTIFICIAL INTELLIGENCE – OPPORTUNITIES AND CHALLENGES IN PROMOTING SECURITY IN INTERNATIONAL POLITICS –

Associate Professor Ecaterina HLIHOR, PhD
"Carol I" National Defence University, Bucharest
DOI: 10.55535/RMT.2024.4.42

Artificial intelligence represents a major technological challenge that creates concerns both in the academic environment and in that of social practice regarding the manipulative nature that some of its applications can have in public diplomacy, when it is subordinated to security. The paper identifies and highlights the possible risks posed by AI through its use by actors seeking to misinform and manipulate public opinion in democratic societies. In the era of AI, the policies, strategies and practices of public diplomacy inevitably change, and this fact will lead to theoretical and methodological developments. The practice of public diplomacy tends to be contradictory due to the objectives pursued, when the security environment is in crisis or even destroyed by the existence of an armed conflict, as is happening today in Ukraine.

Keywords: artificial intelligence; public diplomacy; security; reputational security; information operations;

INTRODUCTION

When John McCarthy first formally proposed the concept of artificial intelligence (AI) at the Dartmouth Summer Symposium in 1956 (Moor, 2006, pp. 87-91), very few political scientists and theorists in communication or in the field of international relations and geopolitics have sensed how much these disciplines will be influenced in theory and in practical activity. The massive penetration of computers and Internet technology into the research and analysis of the international scene, including in the field of communication, has led them to change their position. Today *"Big data"* is seen as an invaluable resource both in the research and analysis of public diplomacy, and in the activity carried out in this field in different countries (Merkouraki, 2024, p. 41). New technologies have often helped manage the complexity of communication in public diplomacy, both in gathering and sharing information. They have simultaneously increased the speed of public diplomacy activities and made the international environment more unpredictable. Artificial intelligence is considered to be one of the biggest technological challenges creating both excitement and concerns about the manipulative nature of some of its applications in public diplomacy (Bjola, Cassidy, Manor, 2019, pp. 83-101). What kind of challenges will public diplomacy face in this world increasingly dominated by artificial intelligence is a question that has generated heated debates among theorists, analysts and practitioners alike, especially since it is connected to the field of security (Pamment, 2024, pp. 49-83). Starting from the premise that the digital revolution in general and AI in particular have already produced a strong impact on public diplomacy, this study is designed to answer the following questions: *Does artificial intelligence play only a positive role in the organization of public diplomacy activities of states in security processes? Does the use of digital public diplomacy in the processes of securing society mean the same for all states today? Is the use of means and tools generated by artificial intelligence leading to a radical change in the principles and practices of traditional public diplomacy?*

The answers to these questions will highlight the opportunities offered by the use of artificial intelligence to make communication with target audiences more effective in public diplomacy. Using the method of comparative analysis and exploring qualitatively the literature such as official policy documents, journal articles, conference proceedings and press articles, it can be established whether

AI has already improved communication in public diplomacy and, if not, how it can do so in the future. At the same time, answering the stated questions, the study will also highlight the possible risks generated by AI through its use by actors who aim to misinform and manipulate public opinion in democratic societies.

THE ROLE OF PUBLIC DIPLOMACY IN SECURING SOCIETY IN THE AGE OF ARTIFICIAL INTELLIGENCE

Public diplomacy, although seen by theorists and practitioners alike as a special activity within the classical diplomacy of states, is part of international political communication in which non-state actors also participate (Ociepka, 2018, pp. 290-303). From this perspective, the activity of public diplomacy is subordinated to the security processes (Gregory, 2005, p. 8) in contemporary society. They comprise "*transmission tools, which extend well beyond traditional media to include social media and other such emerging tools*" (Debray, 2007). According to Nicholas J. Cull, a prominent public diplomacy scholar, this shift is crucial in the information age because the public diplomacy work done by democratic societies today is about more than messages. It aims to build relationships between different audiences, mutual understanding and collaboration. Through this vision and the results obtained in the field of securing and promoting peace in the world, a different kind of security is aimed at, which Nicholas J. Cull defines as *"reputational security"*, a term that in the academic language of Security Studies is not in circulation (yet) in Romania. In his view, this new form of security manifestation is *"a place at the top of the global imagination. Once established, it means that when a challenge comes – whether it comes from a neighbour challenging sovereignty, internal secession, or a natural threat like sea level rise – the world cares"* (Cull, 2019, pp. 9-10). No doubt, this is not a definition in the academic sense, perhaps that is why Cull felt the need to provide other explanations. This time *reputational security* is no longer a place, but *"a quality of security that comes from having a good reputation. And the way to develop that reputation is to be seen as a good country, not just by having a beautiful culture, being a good place to go on holiday, but also by being a moral country, keeping human rights standards, and being part of collective solutions. So, even a relatively powerless country could, by being part of a larger cooperation, having a more widely seen cultural contribution, be valued above its hard power categories"* (Ib.). All these (re)considerations lead to changes in answers to the traditional question: *What is the purpose of a public activity: to inform or to influence?* The possibility arises that the two may be combined, in different proportions, depending on the nature and characteristics of a target audience,

for a set of public diplomacy activities. It aims to inform the public, because public diplomacy activity involves informing about a security aspect/fact, as it happens, in our case, in the *"public affairs"* of government agencies, or even commercial media (Lord, 2009, p. 43). In addition, it must persuade the audience to adopt an attitude and behaviour corresponding to a security process. It means that public diplomacy must not rely on the distortion and manipulation of inconvenient facts to achieve its strategic effect. This truth was validated by the public diplomacy activities carried out by the USA during the Cold War (Hlihor, Hlihor, 2020, pp. 101-121). Much of the power of contemporary public diplomacy in the West can be traced precisely to its well-known commitment to conveying the truth of world events even when promoting a truth through public diplomacy also entails a certain cost. Thus, of central importance to practitioners of American public diplomacy during the Cold War was *"maintaining the <credibility> of their programs – and the success they generally enjoyed in the face of occasional interference from political officials. On the other hand, Soviet information efforts were critically hampered not only by a filter generated by an ideological language increasingly distant from the real world, but also by the routine recourse to classic propaganda techniques, loaded with what the Russian nomenklatura called <disinformation>"* (Lord, p. 48).

Soviet specialists in the field did not understand the difference between propaganda and counter-propaganda, which had as their objective information and disinformation, and public diplomacy, which was engaged in a war of ideas. This is all the more true today, and it is therefore vital that public diplomacy should be correctly used, as modern wars are most often manifestations of wars of ideas. The final victory is not only on the battlefield, but also in the human mind (Reilly, 2009, p. 120).

From this point of view, the representatives of the Copenhagen School are right when they state that security is a socially constructed phenomenon, in other words security is activated, produced, reproduced and maintained through discourse. *"The process of creating security begins with a speech act that must use the rhetoric of an existential threat to emphasize that society is at risk"* (Mijalković, Mančević, 2018, p. 40). It means that the invocation that a referent object (state, society, organization etc.) is threatened is a linguistic construction enunciated by a securitization agent (the representative of a state, of a public institution with security duties, of a commercial company etc.). It becomes a successful securitization process only if a significant public accepts the existence of the threat (Buzan, de Wilde, Waever, 2011, p. 27), thus legitimizing the introduction of exceptional measures

that bypass (pre)established processes to eliminate the perceived threat. In this cycle of perceiving and launching into public opinion threats in numerous fields, such as the study of migration, global environment, critical infrastructure, cyber security and data flows etc., public diplomacy activities can be subsumed under the creation of a desirable security environment. The communication of a security act is no longer done in traditional mass media alone. New media channels are used, including those used by public diplomacy in the age of artificial intelligence.

Today, anyone can access information from any country on the globe if they have a device equipped with a translation engine, but it is not the only facility offered by the digital revolution. AI tools streamline processes and bring operational improvements for public diplomacy practitioners. They are effective for generating media summaries, for example. A chatbot, powered by AI, can function as a virtual assistant to a press officer, interacting with the public, addressing questions, and providing accurate details on government policies and international affairs (Wang, Dubbins, 2024). We will illustrate, by way of example, only one of the opportunities offered by the use of artificial intelligence in public diplomacy activities carried out with the aim of promoting security and cooperation between nations. It refers to the ability of artificial intelligence tools to provide a quick, precise analysis of data regarding the social, cultural, economic, political context, historical psycho-fixations, prejudices in the society where a public diplomacy campaign is to be carried out in favour of security and to make predictions about the evolution trends based on information from the online press and public data about that society. I asked ChatGPT: *"What do the Russians think about Western public diplomacy?"* In less than two seconds, an essential picture of how Russians view Western public diplomacy was drawn:

"Russian opinions on Western public diplomacy are quite varied and often influenced by the broader geopolitical context. Here are some key perspectives:

***1. Scepticism and Distrust**: Many Russians view Western public diplomacy with scepticism, seeing it as a tool for promoting Western interests and values at the expense of Russian sovereignty and cultural identity. This sentiment has been reinforced by historical events and current geopolitical tensions.*

***2. Perception of Bias**: There is a common perception that Western public diplomacy is biased and often portrays Russia in a negative light. This includes media coverage and diplomatic statements that are seen as unfairly critical of Russian policies and actions.*

***3. Impact of Sanctions and Diplomatic Strains:** The imposition of sanctions and the deterioration of diplomatic relations, especially following events like the annexation of Crimea and the conflict in Ukraine, have further strained perceptions. Many Russians feel that Western public diplomacy efforts are part of a broader strategy to isolate and weaken Russia.*

***4. Alternative Narratives**: In response to Western public diplomacy, Russia has developed its own narratives and public diplomacy efforts, focusing on promoting a multipolar world order and countering what it sees as Western unilateralism. This includes engaging with countries in Asia, the Middle East, and Latin America to build alliances and present alternative viewpoints".* (Co-pilot)

This picture can be an excellent starting point for drawing up a working plan of a public diplomacy campaign in contemporary Russian society, if the Russian state were not in the position of aggressor in Ukraine. To the question *"What are some recent examples of tensions between Russia and the West in terms of public diplomacy?"* the co-pilot identified the factors that could hinder a public diplomacy campaign of an institution in a democratic Western country.

"Recent tensions between Russia and the West in terms of public diplomacy have been marked by several significant events:

***1. Ukraine Conflict**: The ongoing conflict in Ukraine remains a major point of contention. Russia's annexation of Crimea in 2014 and its support for separatists in Eastern Ukraine have led to severe diplomatic tensions. The West, particularly the United States and the European Union, has imposed sanctions on Russia, which Moscow views as an attempt to undermine its sovereignty.*

***2. Sanctions and Economic Measures**: In response to various actions by Russia, including alleged election interference and cyberattacks, the West has implemented a series of economic sanctions. These measures have targeted Russian individuals, companies, and sectors, leading to retaliatory actions from Russia.*

***3. Diplomatic Expulsions**: There have been multiple instances of diplomatic expulsions between Russia and Western countries. For example, following the poisoning of former Russian spy Sergei Skripal in the UK in 2018, numerous Western countries expelled Russian diplomats, and Russia responded in kind.*

***4. Media and Information Warfare**: Both sides accuse each other of spreading disinformation and propaganda. Russia has criticized Western media for biased reporting, while Western countries have accused Russian state media of spreading false narratives.*

***5. Military Posturing**: NATO's military exercises near Russia's borders and Russia's military activities in regions like the Arctic and the Black Sea have heightened tensions. Both sides view these actions as provocative and a threat to regional stability.*

These examples illustrate the complex and often adversarial nature of public diplomacy between Russia and the West. Is there a particular event or aspect you'd like to explore further?" (Co-pilot)

How much time and effort must have been invested by a documentary crew to make this image? The answer seems to be a truism, but it cannot be avoided in the age of the digital revolution. Analysing the role of artificial intelligence in the efficiency of public diplomacy activities in the field of security, specialists and analysts from Israel believe that the efficiency of public diplomacy activities through the use of tools offered by artificial intelligence could be manifested on three levels (Barel, 2024). At a strategic level, the use of AI can allow Israel to gain a better perspective on possible future global changes that could influence the balance of world power and affect how Jerusalem will manage its foreign relations, especially with the great powers. At an intermediate level, AI could provide an answer to the existing bureaucratic maze of the public diplomacy system, which often prevents Israeli influence campaigns from working effectively. At the tactical level, AI enables intelligence operatives to respond faster and better to anti-Israel social media attempts to influence disinformation and delegitimization campaigns, including actions that themselves rely on artificial intelligence. The study concludes with a series of recommendations on how the process of absorbing AI in an influence campaign could begin (Ib.).

Another opportunity relates to enhancing the credibility of a public diplomacy activity through the use of AI, especially when it targets an audience in a society that is in a conflict relationship with the country in which the public diplomacy institution is located. AI can provide means of remote interaction, because in such a situation the military and intelligence structures of the target state use all means to prevent such activities. On the other hand, AI uses both overt and covert forms of influence that rely on deception, black and grey forms of propaganda, which affects the ability of public diplomacy professionals to achieve their goals (Gass, Seiter, 2020, pp. 154-165). Some public diplomacy practitioners often wonder how meaningful public diplomacy activities can be created and sustained if the environments they typically rely on become less trustworthy, compromised by artificial intelligence used for deception and disinformation. One possible answer to this challenge is given

by Elizabeth M. Allen, a specialist in strategic communication and public relations in the Obama and Biden Administrations. According to her, artificial intelligence does not fundamentally change the nature and characteristics of public diplomacy: *"We build trust and credibility by doing what we have always done, but better: providing direct, truthful and credible messages, more strategic in our communications. The voice of the United States from the podium and visual branding continues to be effective carriers of information. Investing in audience analytics, focusing on human-centric storytelling, and unifying branding took our messaging even further. Our insightful and creative practitioners in the field add local cultural insight to make our voice even more relevant to our audience. And we are not alone. The smart realignment of our resources around strategic communication has positioned the US government as a key strategic communication partner, creating expertise that government counterparts are eager to learn from and collaborate with. We have built coalitions around trust, coordinating joint statements and strategic messages with partners around the world, from the G7 to the Indo-Pacific Quad and beyond. However, the flag and voice of the US have limits in their reach, especially within closed communication platforms, which is why we also invest in reaching people through credible third parties, stakeholders and influential voices"* (Allen, 2023). None of the public diplomacy theorists are very concerned about the possibility that public diplomacy organizations and institutions in unfriendly countries could undermine the credibility of public diplomacy work by using artificial intelligence. According to Nicholas J. Cull, *"As we move forward to negotiate this digital world, my point is that we shouldn't throw away the lessons of the analog past, and there are some pretty good takeaways from earlier eras of public diplomacy that are recognized as best practices and what has worked in the past will work in the present and in the future because it is based on consistent human beings"* (Cull, pp. 9-10). It does not mean that public diplomacy theorists and practitioners should not research and analyse possible manipulative ways and means of using artificial intelligence. There are still many states on the international stage for whom sowing mistrust is a key objective of their foreign policy. As specialists in the US Department of Defense state, *"information has been turned into weapons, and disinformation has become an incisive tool of state policy"* (British Council, 2022, p. 42). The rapid development of information technologies has created new possibilities for the malicious use of artificial intelligence through strategic deception and psychological warfare operations that pose multiple threats to organizational safety and national security. An extremely large number of fake videos used in such campaigns can be created with the help of artificial intelligence.

THE RISKS GENERATED BY THE ABUSIVE USE OF ARTIFICIAL INTELLIGENCE IN THE ACTIVITY OF PUBLIC DIPLOMACY

Social media and other tools using AI can present a real challenge for public diplomacy practitioners today. Society is increasingly interconnected and there is no to avoid social platforms when you aim to engage in dialogue with a target audience. The first challenge for the *"target"* would be to answer the question of whether the message is built on the basis of information from concrete-factual reality or is generated with the help of artificial intelligence. In other words – to trust or not to trust the sender of a public diplomacy message? The answer is not so simple. Even for a specialist it is difficult to identify who is behind the dissemination of messages, especially in times of crisis and war. In such situations the trail/digital fingerprint of the *"emitter"* can even be blurred to accuse its enemies of deception and disinformation operations, as Russia has often done in the conflict in Ukraine (Kryvenko, 2024). However, not only public diplomacy institutions and organizations in Russia do so. In the case of Russia, it is most obvious, because the specific tools of artificial intelligence are being misused in military-specific operations, which creates great challenges for public diplomacy. Paradoxically, Russian specialists are exploiting precisely the feeling, cultivated in Western public opinion, of trust in the tools and means that use AI for purposes beneficial to society. An edifying example, but not the only one, is ChatGPT which has been widely used in recent years. Professor and public diplomacy specialist Ilan Manor observed that *"The media has portrayed ChatGPT as incredibly smart and sophisticated, so sophisticated that it can pass the bar exam or pass medical licensing exams or pass Ivy League Universities entrance exams. It may cause the public to have <trust> in the information generated by ChatGPT"* (Manor, 2023). He points out that many times *"the answers generated by artificial intelligence can be wrong or misleading"* (Ib.). He illustrates this statement with the answer to the question asked to ChatGPT: *Why did Russia invade Ukraine in 2014?* It offered a short and manipulative answer: *"The invasion was determined by the establishment of a pro-Western government in Kyiv, which threatened the interests of Russia"* (Ib.). It failed to mention that hundreds of thousands of Ukrainians have taken to the streets over several years demanding closer ties with the West, failed to mention that riot police shot and killed protesters, or that Russia's use of digital disinformation and of the armed forces led to the worsening of the internal situation. This fact shows us that trust in such search and analysis engines must contain a dose of caution, because the answers to questions that assume a large analytical load and ethical, political, moral and ideological interpretations

are limited by the information resource stored in such artificial intelligence tools. It depends on who has the interest and ability to *"clutter"* such tools with desirable and interested information. Russia has been doing it for the past 20 years, although initially the reach of its government apparatus for public diplomacy was extended mainly through the mass media (Tsvetkova, Rushchin, 2021, p. 5). In 2005, the TV channel Russia Today was created, followed by the revision of broadcasting agencies, in particular. *"Voice of Russia"* was transformed into *"Radio Sputnik"*. Over time, *"Rossiyskaya Gazeta" ("Russian Gazette")* cooperated with *"The Washington Post", "The Daily Telegraph", "Figaro"* and leading newspapers in Argentina, Bulgaria, Brazil, India, Spain and Italy to publish its articles. Some digital cultural projects also appeared, including Russia Profile, Meeting Russia, and even a social network for graduates of overseas exchange programs. Among the measures aimed at promoting Russian brands abroad were also projects between the Russian government and the American public relations agency Ketchum, which promoted Russian interests within US political institutions (Tsvetkova, Rushchin, ib.). After the Russian aggression on Ukraine, the effectiveness of these public diplomacy activities is practically nil, because *"cross-cultural ties between Russia and the United States are practically frozen. Even Russian specialists admit that Western states have managed to drastically limit the social space in which the Russian Federation could carry out public diplomacy activities and impose its own narratives in relation to the war in Ukraine"* (Burlinova, 2023). They consider 2022 to be a crucial year in reorienting public diplomacy to other regions of the world. According to this approach, public diplomacy must be understood as the sphere of activity of state or non-state actors, whose main task is to establish a dialogue with the target audience of foreign societies, as a rule, in order to achieve national foreign policy objectives (Burlinova, Tabak, 2022). In this situation, Russian officials directed *"all efforts to develop our presence in those countries that perceive Russian public diplomacy as an opportunity to strengthen bilateral dialogue"* (Burlinova, 2023). This aspect shows us that, under the conditions in which Russia was excluded from relations with the West, the essence and character of public diplomacy did not change, but only changed its direction, towards Latin American countries, the Middle East and Africa (Antwi-Boasiako, 2022, pp. 463-482).

Another element that constitutes a great challenge for public diplomacy in the era of artificial intelligence is that of the phenomenon of *fake news* and *deep fake*, especially during wartime (Hlihor, 2024), when the military personnel can also use public diplomacy tools to influence public opinion in the society in which

they act. This is what happened in the war on terror in Iraq and Afghanistan (Wallin, 2015). The war in Ukraine confirmed some of the studies and opinions of specialists who analysed the role of public diplomacy in war situations. Western and Eastern European political elites now widely accept that Russia uses information as a weapon, and that this type of information threatens national security just as much as conventional weapons. The US National Security Strategy, for example, states that *"America's adversaries are weaponizing information to attack the values and institutions that underpin free societies"* (Szostek, 2020, pp. 2728-2748). Moreover, Ukrainians also openly admit that *"public diplomacy is used as a weapon in the war with Russia"* (Kuleba, 2015). Dmitro Kuleba states that *"Where official diplomacy is forced to speak behind closed doors, public diplomacy speaks openly – in conference rooms, galleries, apartments, concert halls, squares and streets. Where the door will not open to official diplomacy, public diplomacy will be hospitably invited to enter. This diplomacy will allow you to keep important foreign policy topics afloat in the sea of hundreds of other topics. Finally, it allows you to reach those who are not interested in public policy, but are interested in open discussion, science, art, texts, music, fashion, food, people and everything called lifestyle. When iron weapons fall silent, soft weapons become even more necessary for Ukraine. The world already knows that Russia is an aggressor state that has destroyed European and international security. The time has come to tell the world, through the tools of public diplomacy, who Ukraine is – a European state with positive changes, freedom and talented people"* (Kuleba, ib.).

In information operations, deception occurs through, among other means, fake news and deep fake. It is difficult to say whether all actors engaged in a conflict use such means in public diplomacy, but the phenomenon cannot be disputed. Professor Corneliu Bjola states that the use of fake news and deep fake constitutes the *"dark side"* of digital diplomacy, because they are disinformation and propaganda tools used by governments and non-state actors in pursuit of strategic interests (Bjola, 2019, pp. 1-2). Easy access to online content creation and editing tools, integration of AI technology in smartphones have paved the way for fraudulent activities such as: creating fake videos, disseminating fake news, disseminating them through social networks. Unfortunately, it has led to blurring the line between subjective comments and verifiable facts. Users often take content with a significant number of likes or reshares on social media as fact without verifying its accuracy. Artificial intelligence has given rise to trolls that can *"mask"* themselves as humans and artificially increase their number of followers, likes and re-shares. Users are more

likely to be attracted to topics that have attracted high engagement, viewing them as valid and trustworthy, thus re-sharing them as real information. Users are constantly bombarded with information and have moved from TV and radio to websites and social media to read news and communicate. Therefore, in an era where *"the news media can be used strategically to take advantage of or increase the uncertainty of the target audience"* it is important to recognize that public diplomacy efforts *"cannot always depend on the construction of stable and positive images of a state or its ambitions"* (Miles, 2021, p. 158).

In order to avoid the negative effects of malicious public diplomacy campaigns, practitioners in the field must find other platforms, different from those that accept such methods to reach the intended audience, while taking into account the challenges and threats of each platform. These are just a few of the challenges and risks posed by AI in public diplomacy work. They are red flags generated by the digital revolution for both practitioners and *"consumers"* of public diplomacy. Society will adapt to all these challenges and exploit everything that is beneficial to it. We do not live in a fundamentally different society compared to previous generations. The perception may be more intense from one age to another. Each generation tends to believe that their own generation is different than the previous generation. This is an ancient human concern and should be seen today as a strategic narrative (Sharma, 2019, pp. 1-6).

CONCLUSIONS

The digital revolution, in general, and artificial intelligence, in particular, have changed especially the practice of public diplomacy when it is subordinated to security, at all levels and of all kinds. Different interests and perceptions of threats, risks and vulnerabilities have made the landscape of public diplomacy activities to shape the attitude and behaviour of a target audience, different from one society to another or from one region to another. The biased mind of communities or individuals accentuates this tendency. An ordinary citizen who is *"caught up"* in a public diplomacy campaign will consume those *"elements"* that suit his/her own beliefs and perceptions from the security environment, and there is a good chance that the particular individual will oppose any content that would have him/her question previous beliefs about a country.

This fact shows us that neither the advantages of using AI in public diplomacy nor the possible risks should be exaggerated. We believe that a comprehensive understanding of public diplomacy policies, strategies and practices – which have

inevitably changed – in the age of AI needs a new theoretical framework to explain their mechanisms and dynamics. The practice of public diplomacy tends to be contradictory especially considering the pursued objectives when the security environment is in crisis or even destroyed by the existence of an armed conflict, as it is happening today in Ukraine. But this fact will not lead to the abandonment of such activities because someone with malicious intent will use one of the AI tools (e.g. ChatGPT) to create and spread fake information online. New technical possibilities to detect them will be identified or, through better education in the digital field, people will reject them as such. Another solution would be to establish rules for the use of AI by both public and non-state institutions. It will not be an easy step to take, because in the commercial/advertising field it is not primarily about ethics and morals, but profit. It could be less difficult to establish norms for the use of AI in the field of security.

BIBLIOGRAPHY:

1. Allen, E.M. (2023). *Public Diplomacy and the Information Space Today. A Strategic Approach*, https://www.aspeninstitute.org/wp-content/uploads/2023/10/Allen_Public-Diplomacy-and-the-Information-Space-Today_Final-Approved.pdf, retrieved on 12 July 2024.
2. Antwi-Boasiako, I. (2022). *The quest for influence: Examining Russia's public diplomacy mechanisms in Africa*, in *South African Journal of International Affairs*, vol. 29, no. 4.
3. Barel, O. (2006). *Artificial Intelligence in the Service of Israel's Public Diplomacy*, *Strategic Assessment*, Policy Analysis, January 2024, https://www.inss.org.il/strategic_assessment/artificial-intelligence/, retrieved on 15 July 2024.
4. Bjola, C. (2019). *The 'dark side' of digital diplomacy: countering disinformation and propaganda*, in ARI5/https://media.realinstitutoelcano.org/wp-content/uploads/2021/11/ari5-2019-bjola-dark-side-digital-diplomacy-countering-disinformation-propaganda.pdf, retrieved on 12 July 2024.
5. Bjola, C., Cassidy, J., Manor, I. (2019). *Public Diplomacy in the Digital Age,* in *The Hague Journal of Diplomacy April*, Brill Nijhoff, retrieved on 12 July 2024.
6. Brandt, J., Schafer, B., Wilson, R.D. (28 September 2023). *A Strategy for US Public Diplomacy in the Age of Disinformation*, Alliance for securing Democracy, https://securingdemocracy.gmfus.org/a-strategy-for-us-public-diplomacy-in-the-age-of-disinformation/, retrieved on 15 July 2024.
7. British Council, *Trust in international relations, public diplomacy and soft power*, *Policy Insight,* https://www.britishcouncil.org/sites/default/files/trust_in_international_relations_public_diplomacy_and_soft_power.pdf, retrieved on 15 July 2024.

8. Burlinova, N. (2023). *Zapad ne priznayet za Rossiyey prava na publichnuyu diplomatiyu*, *Rossiyskiy sovet po mezhdunarodnym delam*/The West does not recognize the right of Russia to public diplomacy. Russian Council for International Affairs, https://russiancouncil.ru/analytics-and-comments/analytics/zapad-ne-priznaet-za-rossiey-prava-na-publichnuyu-diplomatiyu/, retrieved on 20 July 2024.
9. Burlinova, N., Tabak, V. (2022). *Год великого поворота: публичная дипломатия регионов России после февраля 2022 г,* https://russiancouncil.ru/analytics-and-comments/analytics/god-velikogo-povorota-publichnaya-diplomatiya-regionov-rossii-posle-fevralya-2022-g/, retrieved on 20 July 2024.
10. Buzan, B., Wilde, J., Waever, O. (2011). *Securitatea. Un nou cadru de analiza*. Cluj-Napoca: Editura CA Publishing.
11. Copilot, https://www.bing.com/chat?q=the+image+of+contemporary+russian+society&sendquery=1&FORM=SCCODX, retrieved on 20 July 2024.
12. 12.Copilot, https://www.bing.com/chat?q=the+image+of+contemporary+russian+society&sendquery=1&FORM=SCCODX, retrieved on 20 July 2024.
13. Cull, N. J. (2022).*From soft power to reputational security: rethinking public diplomacy and cultural diplomacy for a dangerous age,* https://link.springer.com/content/pdf/10.1057/s41254-021-00236-0.pdf, retrieved on 10 August 2024.
14. Cull, N.J. (2019). *The Tightrope to Tomorrow: Reputational Security, Collective Vision and the Future of Public Diplomacy,* in The *Hague Journal of Diplomacy*, no. 14.
15. Debray, R. (2007). *Socialism: a life cycle*, New Left Review, https://monoskop.org/images/c/c9/Debray_Regis_2007_Socialism_A_Life_Cycle.pdf, retrieved on 10 August 2024.
16. Fjällhed, A. (9 September 2023). *Public Diplomacy in Times of War: Exploring New Ethical Responsibilities in a Shifting Geopolitical Terrain*, The 16th European International Studies Association Pan-European Conference on International Relations, https://portal.research.lu.se/en/publications/public-diplomacy-in-times-of-war-exploring-new-ethical-responsibilities, retrieved on 2 August 2024.
17. Gass, R.H., Seiter, J.S. (2020). *Credibility and Public Diplomacy*, in Nancy Snow, Nicholas J. Cull, eds., Routledge Handbook of Public Diplomacy, 2nd ed., Routledge.
18. Gregory, B. (31 August 2005). *Public Diplomacy and Strategic Communication: Cultures, Firewalls, and Imported Norms*, Paper prepared for presentation at the American Political Science Association Conference on International Communication and Conflict, George Washington University and Georgetown University Washington, D.C.
19. Hlihor, C., Hlihor, E. (2020). *Diplomația publică în confruntarea Est-Vest din timpul Războiului Rece,* in Constantin Hlihor, Bogdan Antoniu, Alin Matei (eds.), Scripta Historica. In memoriam Emeritus Professor Constantin Buse. București: Editura Universității din Bucuresti.
20. Hlihor, E. (2024). *Public Diplomacy in Time of War. Israel's War on Gaza. Case Study*, in *Bulletin of the Transylvania University of Braşov,* Series VII: Social Sciences Law, vol. 17(66), no. 1, https://doi.org/10.31926/but.ssl.2024.17.66.1.13.

21. Interview (26 May 2019). *Scholars' Circle – Emigrant's positive effects on democracy-/-Foundations of Public Diplomacy –*, ScholarsCircle.org., 6 June 2019, https://www.thebigq.org/2019/06/06/qa-getting-the-message-across-what-is-public-diplomacy/, retrieved on 2 August 2024.
22. Kryvenko, P. (2024). *Manipulating Reality: The Role of Social Media. Content and Deepfakes in the Russia Ukraine War,* in *New Geopolitics*, https://www.newgeopolitics.org/2024/03/04/manipulating-reality-the-role-of-social-media-content-and-deepfakes-in-the-russia-ukraine-war/, retrieved on 2 August 2024.
23. Кулеба, Д. (2015). *Публічна дипломатія – нова зброя України в умовах гібридної війни*, în *Європейська правда, Середа,* 23 вересня,https://www.eurointegration.com.ua/experts/2015/09/23/7038633/, retrieved on 2 August 2024.
24. Lord, C. (2009). *What 'Strategic' Public Diplomacy Is*, in J. Michael Waller, ed., *Strategic Influence Public Diplomacy, Counterpropaganda and Political Warfare,* Revised edition, Washington D.C. Crossbow Press.
25. Manor, I. (15 June 2023). *AI's Impact on Public Diplomacy*, *Exploring Digital Diplomacy*, https://digdipblog.com/2023/06/15/ais-impact-on-public-diplomacy/, retrieved on 2 August 2024.
26. Merkouraki, M. (2024). *Turkey's Digital Public Diplomacy in the Age of Uncertainty*, *International Journal of International Relations, Media and Mass Communication Studies*, vol. 10, no. 2.
27. Miles, C. (2021). *The Manufacturing of Uncertainty in Public Diplomacy: A Rhetorical Approach*, in Paweł Surowiec, Ilan Manor, eds., *Public Diplomacy and the Politics of Uncertainty*, Palgrave Macmillan.
28. Mijalković, S., Mančević, M.P. (2018). *Contemporary Security Studies. An Introduction to Methodological, Research and Theoretical Foundations of Security*. Belgrade. Academy of Criminalistic and Police Studies.
29. Moor, J. (2024). *The Dartmouth College Artificial Intelligence Conference: The Next Fifty Years, AI Magazine,* vol. 27, no. 4.
30. Ociepka, B. (2018). *Public diplomacy as political communication: Lessons from case studies*, *European Journal of Communication*, vol. 33, no. 3, March, https://doi.org/10.1177/0267323118763909, retrieved on 4 August 2024.
31. Pamment, J. (2024). *The 'Logics' of Public Diplomacy: In Search of What Unites a Multidisciplinary Research Field*, in *The Hague Journal of Diplomacy*, no. 19.
32. Reilly, R.R. (2009). *Conducting a War of Ideas with Public Diplomacy*, in J. Michael Waller, ed., *Strategic Influence Public Diplomacy, Counterpropaganda and Political Warfare.* Revised ed., Washington D.C. Crossbow Press.
33. Sharma, G.K. (2019). *The Post-Truth Era: An Analysis with Reference to Contemporary Politics*, DLR, 11(1), https://www.dehradunlawreview.com/wp-content/uploads/2020/02/1_The_Post-Truth_Era_An_Analysis-11-16.pdf, retrieved on 4 August 2024.
34. Snow, N., Cull, N.J. (2020). *Routledge Handbook of Public Diplomacy*, 2nd ed., Routledge.

35. Szostek, J. (2020). *What Happens to Public Diplomacy During Information War? Critical Reflections on the Conceptual Framing of International Communication,* in *International Journal of Communication*, no. 14.
36. Tagalog, E.V., Barretto, J.M., Ching, D.L., Paculanan, C. (2022). *Soft power and reputational security: An analysis of the Filipino Erasmus program experience to Poland,* https://animorepository.dlsu.edu.ph/etdb_intlstud/3, retrieved on 10 August 2024.
37. Tsvetkova, N., Rushchin, D. (2021). *Russia's Public Diplomacy: From Soft Power to Strategic Communication,* in *Journal of Political Marketing*, vol. 20, no. 1.
38. Wallin, M. (February 2015). *Military Public Diplomacy. How the Military Influences Foreign Audiences*, https://www.americansecurityproject.org/wp-content/uploads/2015/02/Ref-0185-Military-Public-Diplomacy.pdf, retrieved on 2 August 2024.

CIVILIAN PREPAREDNESS FOR CRISIS SITUATIONS AND THE DEVELOPMENT OF SECURITY CULTURE IN ROMANIA

Student Theodor-Eugeniu MIHAI
"Carol I" National Defence University, Bucharest
DOI: 10.55535/RMT.2024.4.43

The civilian population is an important element for any security system of any given state. It participates, either actively or passively, in crisis situations or conflicts, and the assurance of its general welfare represents a major policy objective. From this point of view, the states have the obligation to prepare the civilian population to anticipate and become aware of the risks and the necessary measures, imposed by the alteration of the overall state of security. The main objective of this paper is to analyse the civilian preparedness and the development of security culture in Romania, from the perspective of the mechanisms, measures and policies implemented in the field by the Romanian state.

Keywords: civilian resilience; security culture; civil-military relation; national security; hybrid warfare;

INTRODUCTION

According to the Convention of Montevideo, the permanent population represents one of the main conditions of statehood (Montevideo Convention on the Rights and Duties of States, 1993). The population contributes, fundamentally, to the functioning of the social and political apparatus, to the economic system, being the main source from which the state derives its sovereign prerogatives. As such, possessing a fundamental characteristic, it cannot be excluded from crisis situations or conflicts that occur upon the state's territory. International law makes a concise distinction between combatants and civilian population. Article 51 of the First Additional Protocol to the Geneva Conventions offers extended protection, from the ban upon indiscriminate attacks to exclusion of civilian population as a legitimate military target (Additional Protocol to the Geneva Conventions, 1977).

The special status granted to them does not completely exclude the civilian population from a conflict. Civilians can act and participate by supporting the state's efforts without losing their non-combatant status. In this regard, the European Union's sanctions packages against Russia are notable. They include sanctions on civilian companies in aviation, transportation, gas, and oil, as well as on individuals involved as non-combatants who provide material support or promote state propaganda (Farmer, Booth, Karaman, 2024).

The evolution of hybrid warfare in recent years has accelerated the involvement of civilian population, currently, with hostile actions increasingly directed at the civilian sector rather than defence institutions. As such, the civilian population becomes a target and a means of defence through ensuring unity, homogeneity and by commitment to each individual role, within the framework of the state.

Starting from the importance of civilian population in ensuring national security, the purpose of this paper is to evaluate the level of preparedness in critical situations for the accomplishment of general resilience of the state. Security culture is relevant because it represents an effective tool to create an advanced level of consciousness within the civilian population, thus offering the civilians the capacity and necessary information. The main goal of the security culture is the preparation of civilians

to defend the national values against a potential adversary. The civilian population requires a high level of knowledge, as to act pro-actively and to streamline the state's intervention in times of crisis or conflict.

CURRENT STATE OF CIVILIAN POPULATION PREPARATION AND SECURITY CULTURE IN ROMANIA

The Romanian State has become aware of the importance of civilian population and the role that civilians have in maintaining security and preventing crisis situations or conflicts. It is remarked that, within the *National Defence Strategy for the 2020-2024 period*, one of the action lines for crisis management is presented as follows: *"Preparing institutions and the population for crisis situations and civil emergencies, including through the conduct of exercises and mobilization training, as well as through international cooperation"* (Strategia Națională de Apărare a Țării, 2020, p. 36). From this point of view, the preparation of civilian population and, also, of relevant institutions represents the means to achieving the national security objectives and the country's defence.

It is important to add the fact that the security culture aspect has been covered, being affirmed as a capability of resilience, its development being of absolute necessity for the integration of national security values (Ib., p. 10). The low level of security culture is presented as a vulnerability, its absence making the interference of hostile entities possible (Ib., p. 29). As such, the decision-making apparatus remarks the lack of a satisfactory security culture level of the population.

To understand the necessity of a security culture, it is essential to present the definition provided by the Guide of the National Defence Strategy from 2015, which is also used for the present document: *"[...] the totality of values, norms, attitudes, or actions that determine the understanding and assimilation of the concept of security and its derivatives at the societal level (national security, international security, collective security, insecurity, security policy etc.)"* (Ghidul Strategiei Naționale de Apărare a Țării, 2015, p. 7).

Likewise, it must be mentioned that the notion of security culture has a purely educational dimension, representing the capacity for awareness and the application of an appropriate attitude aimed at contributing to the prevention of insecurity situations and the defence and protection of oneself, one's property, the community, and, obviously, the state as a whole. The Guide affirms the importance of security

culture and the awareness of security elements by the civilian population, elements which are absolutely necessary for maintaining internal security (Ib.).

Another important element of the National Defence Strategy's Guide is the introduction of the *extended national security* – a concept that is used by both the 2015 Strategy and the present one. From this point of view, the decision-makers have observed a need for differentiating between the terms of security and defence, whose distinctions are not explained in detail, but merely state the presence of some unexplained differences. The role of *extended national security* is to replace the strategic univalence of the term *"security"*, which was associated, strictly, with territorial defence, with the objective of extending the notion of security in wider spheres such as: economy, health and transportation (Ib., p. 13).

This aspect creates more issues, in theory, because the terms *"security"* and *"defence"* have clear conceptual delimitations and the integration of both in an unitary form could create more confusion regarding theory. However, this new term creates a new value for the civilian population. Affirming the extension of the notion of *"security"* over other environments, it means that the mentioned institutions, which are not specialized in this aspect, will participate directly in the process of maintaining security. From this point of view, the need for security culture development and the preparedness of civilian population for situations of insecurity, crisis or conflict is even more necessary.

Law no. 481/2004 regarding civilian protection envisions in article 3, letter C: *"Informing and preparing the population in advance regarding the dangers they are exposed to, the self-protection measures that must be taken, the available protection means, the obligations they have, and the actions to be taken during an emergency situation"* (*Legea nr. 481 privind protecția civilă,* 2004, p. 1).

The citizens receive a series of obligations in regards to civilian protection, according to law, such as: complying with the rules established by local or central authorities, taking civilian protection measures, allowing the access of the forces and the means of intervention within the boundaries of one's property, executing emergency evacuations from affected areas etc. (Ib., p. 7).

Irrespective of their status, according to the Constitution of Romania, each citizen is obliged to participate in the country's defence process (Constituția României, 2003, p. 23). As a consequence, the civilian population requires preparation from the state. Considering that the extended national security covers a large area

of fields from health, to economy and to the cyberspace – it is to be noted that while they are integrated actors of the security system, a large portion of the population is not specialised for this purpose.

The Department for Emergency Situation within the Ministry of Internal Affairs implements collaborative projects regarding civilian population, co-operating with the local population, non-governmental organisations and the private sector. These projects stipulate a series of exercises, considering the population's mentality during emergency situations, the continuation of governance, and testing reaction time. They are intended to contribute to the civilian resilience development, improvement of professional preparedness as well as to observe vulnerabilities, gaps or issues (Department for Emergency Situations*, Civil-Military Cooperation in the Field of Civilian Protection and Emergency Management,* 2021).

A concrete example is represented by the *Seism 2018* exercises, organized by the Ministry of Internal Affairs through the Department of Emergency Situations. The exercise's scenario is based upon a hypothetical earthquake with a magnitude of 7.5 Richter, in Vrancea county, which has produced ample material destruction – from administrative buildings to critical infrastructure. Within the *Seism 2018* exercise, the Defence Staff actively participated by engaging 1,000-strength military personnel. The specific missions of the exercise included the installation and operation of campaign hospitals, medical evacuations, identification of material losses and victims (Exercise *Seism 2018*, Agenția Media a Armatei, 2018).

Regarding security culture, the Romanian Intelligence Service promotes a series of prevention and intervention programs such as: *"Radicalisation Awareness Network, Community Policing Preventing Radicalisation, CLEAN-IT, First Line Against Radicalisation"* (Stan, Stăiculescu, Predoană, 2023 pp. 83-84). These programs have the main purpose to curb radicalism and terrorist ideologies through prevention, detection and information. For example, *CLEAN-IT* works with eliminating terrorist activities from the on-line channels within the European Union. *"First Line Against Radicalisation"* oversees the training of police officers to properly detect radicalised individuals (Ib.). Actions regarding security culture development could be put in motion by other state institutions, governmental and non-governmental organisations, educational institutions, as long as they are supervised and coordinated by the Supreme Council for the Country's Defence (Mantea, 2019, p. 202).

To maintain a connection between civilian population and state institutions that are relevant for crisis and conflict situations (such as the Ministry of Internal Affairs, the Ministry of National Defence, the Romanian Defence Staff etc.), they use strategic communication and public information structures, through media (Ib., pp. 201-202). In practice, the preparation of civilian population regarding defence is mentioned in article 2, paragraph 1 of Law no. 446/2006: *"The preparation of Romanian citizens for defence represents the totality of measures and actions taken to ensure the human resources necessary for the armed forces and other forces provided by public defence, public order, and national security institutions, according to the law, hereinafter referred to as institutions with responsibilities in the field of defence and national security. This includes recruitment, selection, training, and assignment to the units of the respective institutions"* (*Legea actualizată nr. 446/2006 privind pregătirea populației pentru apărare,* 2012). In this regard, the law affirms through article 2, paragraph 2, that the civilian preparedness can be realised through two means: *"a) fulfilling military service; b) participating in other forms of training organized by the country's defence and national security institutions"* (Ib.)

A main issue in regards to this law is its topicality, the last modification occurring in 2012. The conflictual phenomenon has been modified, including more profoundly the civilian element and the non-military side. As such, I consider that there is a need to update it to include civilian preparedness for resilience against hybrid attacks.

THE LEVEL OF SECURITY CULTURE – A VULNERABILITY

As mentioned in the *National Defence Strategy for the 2020-2024 period*, it is considered that the security culture low level constitutes a vulnerability, in regard to disinformation and hostile hybrid actions. In this context, it is necessary to analyse the current level of security culture to understand how problematic this issue is. In this regard, the National Strategy lacks a wider perspective. Even if some works that analyse the level of security culture utilise, as a main source, the LARICS Security Culture Barometer (Mantea, ib.; Nistor, 2023), it can be considered outdated. From 2018 until present, the Romanian society has been challenged with internal problems and external ones as well. The COVID-19 pandemic and the Russo-Ukrainian war have led to a shift in perception, and as such the 2018 Barometer cannot accurately reflect the reaction and the views of Romanian citizens regarding the new security problems.

One of the main issues regarding the development of security culture is represented by the citizens' lack of trust in the principal media sources and those of the state institutions, as civilians begin to adopt a conspirative attitude, perceiving the internal and external actions of the Romanian state and its allies with a somewhat, degree of paranoia and scepticism (Nistor, p. 100).

A study conducted between April and October 2020 shows that the population's satisfaction towards the actions taken by the state and the support towards the government has significantly lowered. The context of the analysed period was represented by the peak of the COVID-19 pandemic in Romania. In October 2020, 59.9% of the population showed dissatisfaction with the measures taken by the government and 42.2% of the population had no support for the government (Radu, 2021, pp. 134-135).

Regarding the international conflicts, such as the ones in Ukraine and Gaza, INSCOP conducted a study in December 2023. An important point is represented by the responsibility for the Ukrainian War – only 49.8% considered that Russia is to be blamed, while 28% considered that NATO, Ukraine or the United States of America were the ones guilty of aggression (INSCOP, 2023). The same study shows that only 50.5% of the interviewed Romanians would be willing to defend their country, while 11.8% affirmed that they would hide until the cessation of the conflict, 19.4% would emigrate and 5.6% declared that they would discharge a medical certificate attesting their incapacity and lack of abilities to participate in the defence of the country (Ib.). This aspect is problematic because defence is not provided only by the responsible structures and institutions, but, as national security, it is provided through the unity and total involvement of the Romanian citizens. The fact that 36.8% of the interviewed affirmed they would seek fraudulent means to be relieved of a constitutional duty is a major issue. As such, the lack of security culture and the lack of understanding with regard to individual roles could transform, in the future, into an issue of human resources. This fact is shown in the new recruitment wave of the National Defence Ministry. From the 5,093 positions for professional soldiers, only 40% have been occupied. Moreover, for the mentioned number of positions, only 6,448 candidates presented. From this pool, 24% were rejected for failing the physical aptitudes test and 18% were rejected for failing the psychological examination (*Elemente din analiza procesului de angajare în armată a soldaţilor profesionişti*, Ministerul Apărării Naționale, 2024).

It is to be remarked that, besides the low number of candidates, the quality of those present was unreliable. The issue of human resources in the field of defence is a topical problem that will deepen, in the near future, in terms of both quantity and quality. In this context, new measures for developing security culture and measures for modelling the population to achieve the necessary capacity for defence become imperatives of the Romanian state.

The perspective of citizens towards Romania's foreign policy represents another vulnerability generated by the lack of security culture. As such, a study conducted by INSCOP in May 2024, shows that 27.7% of those questioned affirmed that Romania's ascension to the European Union was, rather, a disadvantage. Another segment of 42.3% sustained the fact that the Romanian Members of the European Parliament should fight for equal rights between Romanian citizens and the rest of the European Union's citizens, through this affirmation implying the fact that there are inequalities among the citizens of the European Union, from the perspective of political representation (INSCOP, 2024).

Another problem is represented by the lack of public information about the attributes of the European Union. A major segment of 73% affirms that they are not informed regarding the activity of Romanian Members of the European Parliament, 72.3% lack information about the activities of the European Parliament, 74.1% lack information about the activity of the European Commission (Ib.).

Lack of public information allows for the popularisation and interiorisation of Euroscepticism and hostile propaganda meant to destabilize the relations between Romania and its allies, this phenomenon being generated, directly, by the lack of security culture.

NATO PERSPECTIVES AND APPROACHES ON CIVILIAN PREPAREDNESS AND SECURITY CULTURE

In the North Atlantic Treaty, article 3 stands as a reference for the strategic resilience of the Alliance: *"In order more effectively to achieve the objectives of this Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack"* (The North Atlantic Treaty, 1949). As such, this principle shows the duties of NATO states to guarantee their own resilience against attacks and shocks, including, also, the preparedness of civilian population for such

events. Resilience, in this sense, refers to the individual and collective capacity of the states to deter any disruption or shocks. Collective resilience is built through the capacity for defence as well as through the preparation of civilian population. The role of civilian capacity is to ensure the stability and security of the measures and actions taken by the states to maintain the guarantees of the North Atlantic Treaty (Strategic Warfare Development Command, 2023).

After the end of the Cold War, the North Atlantic Treaty Organisation has raised the degree of cooperation between the political-military structures and the civil ones. At present, the Alliance is bound to the civilian means and their capacity to support the efficiency of military forces. For example, 90% of military transport for operations is maintained by the civilian commercial sector: 70% of the satellite communications used for defence belong to commercial operators; 95% of the Transatlantic internet traffic, which also includes military communications are offered by private-owned network services (Civil-Military Cooperation Centre of Excellence, 2018, pp. 2-3).

The private sector is a key element for civilian preparation for resilience, NATO thus building long-term partnerships between its institutions, the states and the private sector. As such, the member states are required to develop and consolidate relations with the private sector, to promote collaboration and to communicate the vulnerabilities and the societal risks, in their entirety (Ib., p. 6).

From the perspective of the Alliance, civilian preparedness begins at an individual level. Individual civilian preparedness consists in ensuring the capacity to act towards the consequences of an unfavourable event, of a critical situation or of a major crisis. The key means to ensure individual security are general knowledge, capacity to ensure survival and maintaining a line of communication with the main authorities (Ib., p. 7).

CONCLUSIONS

Highlighting the strategic importance of civilian preparedness and security culture, these aspects are essential both nationally and collectively, contributing to the overall resilience. Romania has the necessary legal framework to implement measures that could enhance both the preparedness of its population and its security culture. However, in practice, these measures remain superficial, serving mostly an informational function without substantial impact. There are exposed

vulnerabilities caused by the public's lack of trust in the state, scepticism toward the measures adopted during crises, and the reactions of the citizens in relation to the benefits derived from Romania's foreign policy and its international commitments.

One acceptable solution is for the new National Defence Strategy to include among its national security objectives the assurance of resilience through civilian preparedness and the development of security culture. It should outline key action plans and create measures that, through a synergistic effect, would provide the civilian population with the necessary materials for preparedness, understanding, and awareness of their role within national security and territorial defence. Civilian preparedness and security culture can also be approached collectively within NATO by establishing a bridge between civilian institutions whose responsibilities are critical during crises or conflicts. Furthermore, a common platform for promoting security culture could be developed.

In the 21st century, security culture is becoming increasingly relevant, particularly in the face of hybrid actions carried out by hostile states and organizations. With the globalization of communication and public media, it can be achieved more easily, as media channels can be used to inform citizens and highlight the significance of these issues. From the population's perspective, the Romanian state must ensure the necessary demographic to secure the human resources for military resilience and territorial defence. The current quantitative and qualitative gaps, along with the lack of interest in national security and defence, are driven by a deeply low level of security culture. By fostering a deeper understanding of general security concepts, individual roles, and each citizen's obligations, the quality and quantity of the country's human resources could be significantly enhanced.

BIBLIOGRAPHY:

1. Agenția Media a Armatei (2018). *Exercițiul Seism 2018,* http://presamil.ro/exercitiul-seism-2018/, retrieved on 20 October 2024.
2. Civil-Military Cooperation Centre of Excellence (2018). *Resilience through Civil Preparedness. Concepts, Interoperability and Capability Branch,* https://www.cimic-coe.org/resources/fact-sheets/factsheet-resilience-through-civil-preparedness.pdf, retrieved on 18 September 2024.
3. *Constituția României/Constitution of Romania* (2003), https://www.ccr.ro/wp-content/uploads/2020/03/Constitutia-2003.pdf, retrieved on 20 October 2024.

4. Department for Emergency Situations (2021). *Civil-Military Cooperation in the Field of Civil Protection and Emergency Management*, https://www.project-engage.eu/civil-military-cooperation-in-the-field-of-civil-protection/, retrieved on 1 September 2024.
5. Farmer, S., Booth, M., Karaman, I. (2024). *EU's 14th Package of Sanctions on Russia*, https://www.globaltradeandsanctionslaw.com/eus-14th-package-of-sanctions-on-russia/, retrieved on 20 October 2024.
6. *Ghidul Strategiei Naționale de Apărare a Țării pentru perioada 2015-2019/National Defence Strategy Guide* (2015). București: Administrația Prezidențială.
7. *Informarea cu privire la activitatea instituțiilor europene.* https://www.inscop.ro/wp-content/uploads/2024/05/9.05.-INSCOP-News.-Perceptie-UE.pdf, retrieved on 16 September 2024.
8. INSCOP. (2023). *Opiniile românilor despre războiul din Ucraina, conflictul Israel – Hamas, apartenența la NATO și UE,* https://www.inscop.ro/decembrie-2023-sondaj-de-opinie-inscop-research-la-comanda-new-strategy-center-opiniile-romanilor-despre-razboiul-din-ucraina-conflictul-israel-hamas-apartenenta-la-nato-si-ue/, retrieved on 15 September 2024.
9. INSCOP (2024). *Avantajele apartenenței la UE, prioritatea viitorilor europarlamentari români.*
10. *Legea actualizată nr. 446 din 30 noiembrie 2006 privind pregătirea populației pentru apărare/Law no. 446 on 30 November 2006 regarding the civilian preparation for defence (updated)* (2012), https://legislatie.just.ro/Public/DetaliiDocument/77597, retrieved on 9 September 2024.
11. *Legea nr. 481 din 8 noiembrie 2004 privind protecția civilă/Law no. 481 on 8 November 2004 regarding civilian protection* (2004). București: Parlamentul României.
12. Mantea, P.D. (2019). *Security Awareness in Romania – Security Culture and Social Responsibility Development Pillar*. Land Forces Academy Review, vol. XXIV, 3(95). DOI: 10.2478/raft-2019-0023.
13. Ministerul Apărării Naționale (2024). *Elemente din analiza procesului de angajare în armată a soldaților profesioniști,* https://www.agerpres.ro/comunicate/2024/04/22/comunicat-de-presa-ministerul-apararii-nationale–1284676, retrieved on 16 September 2024.
14. *Montevideo Convention on the Rights and Duties of States* (1933), Montevideo, https://www.ilsa.org/Jessup/Jessup15/Montevideo%20Convention.pdf, retrieved on 20 October 2024.
15. Nistor, D.I.A. (2023). *Manifestations of security culture at national level*. In *Bulletin of "Carol I" National Defence University,* București, no. 2/2023. DOI:10.53477/2284-9378-23-22.
16. *Additional Protocol to The Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts* (1977). New York, https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.34_AP-I-EN.pdf, retrieved on 20 October 2024.

17. Radu, B. (2021). *Trust in public institutions and compliance with measures against the COVID-19 Pandemic. Case Study on the Metropolitan Area of Cluj, România*. In *Transylvanian Review of Administrative Studies*, no. 63/2021, pp. 128-150. DOI: 10.24193/tras.63E.7.
18. Stan, B.-E., Stăiculescu, A.-R; Predoană, M.-R. (2023). *Strengthening the Security Culture in Romania*. In *Romanian Intelligence Studies Review* 1(29). ISSN-2393-1450.
19. *Strategia Națională de Apărare a Țării pentru perioada 2020-2024/National Defence Strategy 2020-2024* (2020). București: Administrația Prezidențială.
20. Strategic Warfare Development Command (2023). *Resilience and Civil Preparedness in NATO*, https://www.act.nato.int/article/resilience-and-civil-preparedness-in-nato/, retrieved on 18 September 2024.
21. *The North Atlantic Treaty* (1949). Washington D.C., https://www.nato.int/cps/en/natohq/official_texts_17120.htm, retrieved on 18 September 2024.

MILITARY MOBILITY IN THE VISION OF NATO AND EUROPEAN UNION

Major Associate Professor Tiberiu GIURGIU, PhD, BEng

Colonel Associate Professor Ioan VIRCA, PhD, BEng

Lieutenant Gabriel NOJA, BEng, PhD Candidate

"Nicolae Bălcescu" Land Forces Academy, Sibiu

DOI: 10.55535/RMT.2024.4.44

Military mobility in the Euro-Atlantic context is an essential strategic element for strengthening regional and global security, aiming to facilitate the rapid and efficient transport of forces and equipment between NATO and EU member states. In this regard, recent investments have focused on upgrading infrastructure and simplifying cross-border procedures to enable the effective deployment of forces in emergency situations. The projects initiated and managed by the European Defence Agency or under the PESCO umbrella in recent years, which aim to increase the functionality of military mobility corridors, connecting nations in Europe through logistics hubs, contribute to improving interoperability and rapid reaction in the context of current security challenges. Such a multinational logistics network optimizes the use of existing resources, with a focus on the development of dual-use (civil-military) transport infrastructures, while supporting preparedness for possible operations and increasing responsiveness and sustainability in the face of threats.

Keywords: military mobility; dual-use infrastructures; logistics; NATO; EU;

INTRODUCTION

Military mobility in the Euro-Atlantic space is a central pillar for ensuring collective security and defence in the face of global threats. The need for significant investments and the implementation of strategic projects has become more evident in the context of rising geopolitical tensions, especially after Russia's invasion of Ukraine. The effective mobility of troops and military equipment ensures a rapid response in the event of a crisis, allowing the deployment of resources in strategic areas, thus strengthening the deterrence capacity of NATO and the EU (Usewicz et. al, 2022, p. 15).

In this context, investments in transport infrastructure, such as the modernization of road, rail and air networks, are essential to reduce reaction time and optimize cross-border mobility. Such initiatives bring major benefits, including increased responsiveness, reduced bureaucracy and strengthened supply chains. However, challenges remain, including legislative barriers and inadequate infrastructure in certain regions.

Recent conflicts, in particular the one between Russia and Ukraine, underline the need for flexible and efficient logistical capabilities. In this context, opportunities to strengthen military mobility are expanding, through greater coordination between member states and through the integration of new technologies. These efforts will not only strengthen collective defence but will also improve the ability to react to new security challenges. The concept of *collective defence* is not a new idea, being a response to the growing threats and vulnerabilities of states. Article IV of the Treaty of Brussels (2018) and Article 5 of the Treaty of Washington (1949) explicitly provide for the obligation of signatory states to provide mutual assistance in the event of aggression, aiming to restore security. The implementation of this mutual support involves the mobilization of the military structures of the partner countries, generating multiple legislative and procedural implications. A detailed analysis of transit zones and the efficient use of transport infrastructure is needed, having a direct and significant impact on military mobility. These issues are priorities on the European agenda, and the ultimate objective of these efforts is to ensure security in the European space (Gheondea et. al, 2022, p. 45).

The paper therefore aims to highlight the main measures that NATO and European Union member states are considering to streamline military mobility in the Euro-Atlantic space. Moreover, the main projects and initiatives meant to contribute to the realization of this goal are presented, emphasizing the opportunity and benefits of investments in the modernization and development of land, sea or air transport infrastructures with dual civil-military use. Romania's position and the measures taken at national and international level in the context of streamlining military mobility are also presented in this paper.

MILITARY MOBILITY IN NATO'S VISION

Military mobility is seen by NATO as a key factor for rapid force projection, collective defence and deterrence of emerging threats and it is necessary to create an integrated and well-regulated framework to ensure effective and coordinated defence against current threats, especially in the context of recent crises and conflicts. Therefore, NATO pays particular attention to improving transport and logistics capabilities, interoperability between allies, and removing administrative and physical barriers.

NATO stresses the need for military forces to be able to move rapidly over long distances, both within Europe's borders and to crisis areas. It is vital to respond to unexpected threats and to support allies within the margins of Article 5 of the Washington Treaty (collective defence). Improving transport infrastructure and adapting it to military requirements are priorities to enable the rapid movement of troops, military equipment and heavy equipment.

NATO also emphasizes interoperability, consisting in the ability of forces from different member states to operate jointly, using compatible procedures, equipment and systems. Close cooperation between NATO and the European Union is essential in this regard, in particular through joint programs, such as the *Military Mobility Initiative*, which aims to simplify and harmonize military transport procedures between NATO and the EU member states.

Another major objective is to remove administrative and logistical barriers that can delay or even prevent the rapid movement of troops and equipment. The aim is therefore to simplify these procedures, by obtaining border crossing permits quickly and reducing waiting times at borders. Work is being done to standardize documentation and harmonize military transport rules between NATO countries to ensure maximum fluidity in the movement and transportation (M&T) sector.

Equally, NATO stresses the need to strengthen critical infrastructure, referring to roads, bridges, ports and rail networks, to withstand the weights and dimensions of military equipment. In addition, the infrastructure must be resilient to cyber or physical attacks, which could disrupt logistics chains. The ability to protect transport routes and quickly restore damaged infrastructure during conflicts is also very important.

MILITARY MOBILITY IN EU'S VISION

Political-socio-economic developments at European level have led the European Commission to accelerate the implementation of integration measures within the European military mobility project. The current geopolitical situation, generated in particular by the Russian Federation's aggression against Ukraine, underlines the need for the EU to take concrete and targeted measures in key areas to achieve its objectives. As a result, the EU has been and is continuously forced to revise its strategic vision on military mobility, which represents an essential topic for the defence and security of the entire European Union and beyond (Bangală, 2023, p. 385).

Figure 1 shows a SWOT analysis (Chihaia, 2023, p. 5) on military mobility in Europe. This analysis reflects the need to continue and concretize the recent initiatives in the field of military mobility, so that the existing documents and commitments expressed between the various NATO and/or EU member states do not remain at the stage of a general framework but even produce beneficial effects on military transports. A key element in this approach could be investments in the modernization and development of dual-use, civil-military infrastructures, thus generating a streamlining of transport and an optimization of long-term logistics flows, both in peace and in crisis or war situations.

Optimizing supply chains at EU level can also support military mobility by reducing transport times, coordinating resources efficiently and improving logistical capabilities for fast and efficient operations. By integrating national and multinational supply chains, European states can ensure a rapid and continuous flow of equipment, ammunition and supplies, regardless of the location of military units. Better coordination of logistics networks and distribution centres, including using shared logistics hubs, can reduce the time needed for procurement and deployment. In addition, by integrating modern technologies, such as digital supply chain management systems, military transport flows can be optimized,

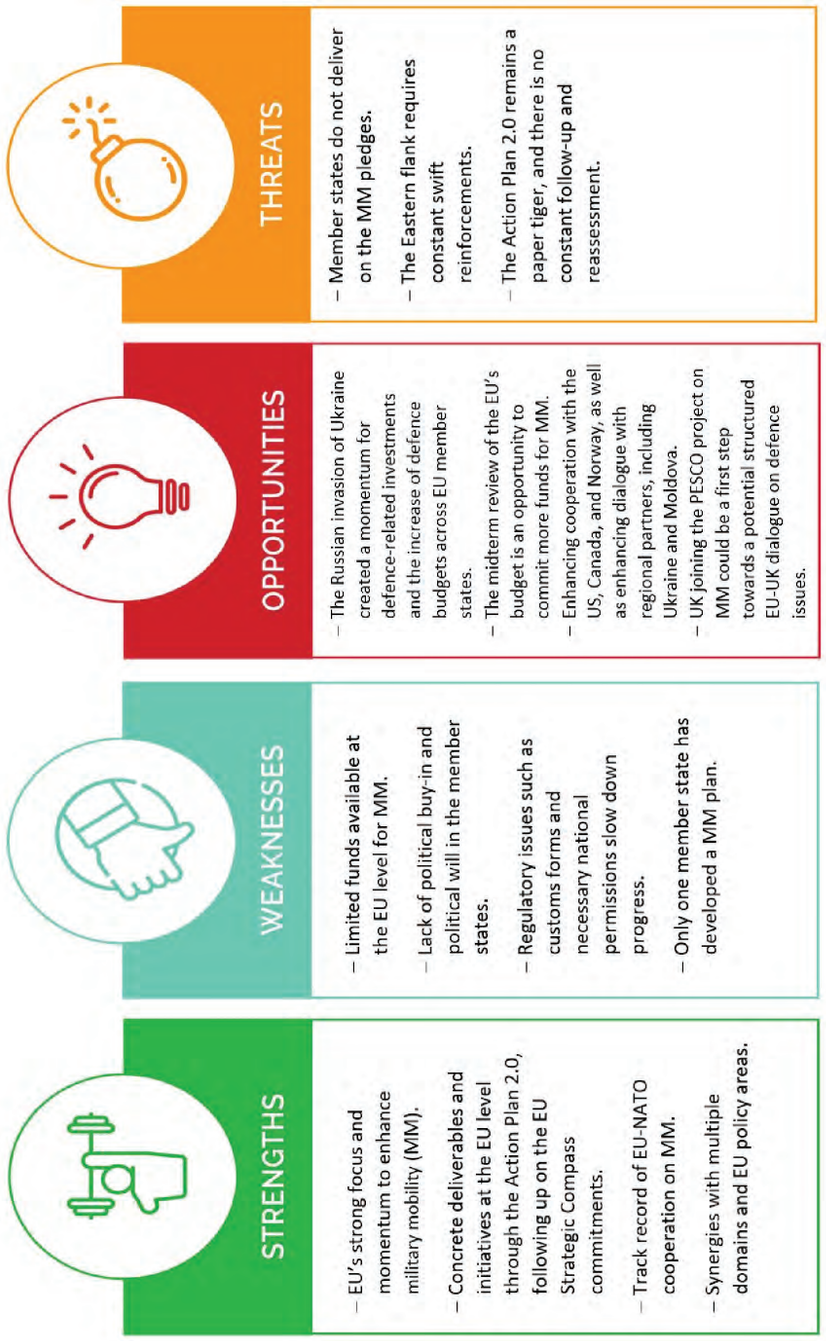


Figure 1: SWOT analysis on military mobility in Europe (adapted after Chihaia, ib.)

thus contributing to the efficiency of logistics (Minculete et. al., 2022, p. 6). These technologies allow for more accurate equipment tracking, real-time inventory management, and better coordination between supply points, leading to efficient resource distribution.

Action Plan on Military Mobility 2.0

The EU's *Action Plan on Military Mobility 2.0* (APMM 2.0), launched in November 2022, was developed within the framework of the European Defence Agency (EDA) and represents an initiative aimed at improving the European Union's ability to quickly and efficiently transport military forces and equipment on European territory, both for common defence operations and for international missions (Gheondea, Pleșanu, 2022, p. 47). This document is a continuation and extension of the first military mobility plan launched in 2018.



Figure 2: Main axes of the EU Action Plan on Military Mobility 2.0 (authors' design)

Figure 2 summarizes the five main axes on which the major objectives of APMM 2.0 have been outlined. Specifically, these objectives consist of:

❖ *Improving critical infrastructure*, both by adapting transport infrastructure (roads, railways, ports and airports) to support specific military mobility needs, including strengthening bridges and adapting gauges to support heavy military

vehicles and equipment, and identifying and correcting shortcomings in the trans-European transport network (TEN-T), so that it ensures good civil and military mobility.

❖ *Simplifying border crossing procedures*. It can be achieved by reducing the bureaucratic and legal barriers that hinder the rapid transport of troops and equipment between member states, respectively by creating harmonized procedures for granting transit permits and developing a *"Military Schengen"* for more efficient military mobility.

❖ *Civil-military coordination*. Collaboration between the civilian and military sectors is considered necessary to use the available infrastructure and resources effectively and to meet the needs of both areas. Equally, a potential solution would be to mobilize financial resources from civilian budgets, such as the Connecting Europe Facility (CEF), to support investments in critical infrastructure for military mobility.

❖ *Increased cooperation with NATO and international partners*. The action plan stresses the need to ensure interoperability and coordination between the EU and NATO in the field of military mobility, to avoid duplication of efforts and ensure coherence in strategic planning. At the same time, expanding cooperation and partnerships with third countries, especially those in the Eastern Neighbourhood and the Western Balkans, is an important objective for improving military mobility in Europe.

❖ *Improving resilience and crisis preparedness*, both by increasing the EU's capacity to respond quickly to crises and security threats, and by ensuring rapid and effective military mobility in the event of emergencies or conflicts. Moreover, it is necessary to integrate military mobility into defence and cybersecurity plans to ensure the security of operations.

The APMM 2.0 therefore aims to transform Europe into a better defence-ready *"strategic area"* and to increase the EU's ability to react quickly to security threats, both at European and global level. It promotes synergy between civilian and military infrastructure, aims to simplify administrative procedures and intensifies collaboration with NATO and other international organizations.

PESCO Initiatives in the Field of Military Mobility

Between 2021-2022, Norway, Canada, the US and the UK joined a cooperation program called *Military Mobility (MM),* under the umbrella of the Permanent Structured Cooperation (PESCO). *"The stated aim of the project is to support Member States' commitment to find ways to simplify and standardize cross-border military transport procedures, aiming to allow the unhindered movement of military personnel and goods within the EU's borders, by road, sea, rail or air, without lengthy bureaucratic procedures"* (Bangală, p. 387). The project is coordinated by the Netherlands, and among the member states participating in the project are the USA, Canada, Norway, Austria, Belgium, Italy, Spain, Canada, the Netherlands, France, Croatia, Hungary, Slovakia, Slovenia, Poland, Romania, Bulgaria, Portugal, Greece or Cyprus.

Another project carried out via PESCO is the *Network of Logistic Hubs in Europe and support to operations (NetLogHubs)*, which aims to create a multinational network based on existing logistics capacities and infrastructure. The main objective is to use a network of existing logistics facilities for multinational operations, prepare equipment for missions, share storage space for spare parts or ammunition, and harmonize transport and deployment activities. Nations in Europe will provide their own capacities so that more logistics hubs can be used. Connected with the European Multimodal Transport Hub, which provides the lines of communication between multinational hubs, the network will grow to cover the entire continent. As for possible operations, for the pre-movement of materials, warehouses and maintenance facilities of other European countries could be used for each other. The network will reduce reaction time and increase capabilities and sustainability for military operations. The project is coordinated by Germany, and the member states participating in the project include Belgium, Italy, Spain, Canada, the Netherlands, France, Croatia, Hungary, Slovakia, Slovenia, Poland, Bulgaria or Cyprus.

Investments in Euro-Atlantic Dual-use Infrastructure

According to an analysis (Chantraine, 2024, pp. 9-11) presented at the *Dual Use & Military Mobility Seminar* held in Ghent, Belgium, on 23 February 2024, after 3 submission sessions, 95 projects aimed at infrastructure investments initiated by 21 member states were funded. The funded projects aim at the modernization and development of dual-purpose infrastructures and cover all means of transport,

namely by land (road and rail), by air and by water (sea and river). *Figure 3* shows a summary of the investments made by member states in the 3 project submission sessions, by transport category. Analysing the data provided, approximately 50% of the investments are aimed at railway infrastructure, 31% at road infrastructure, the remaining 19% being allocated to infrastructures that support military transport by air and water.

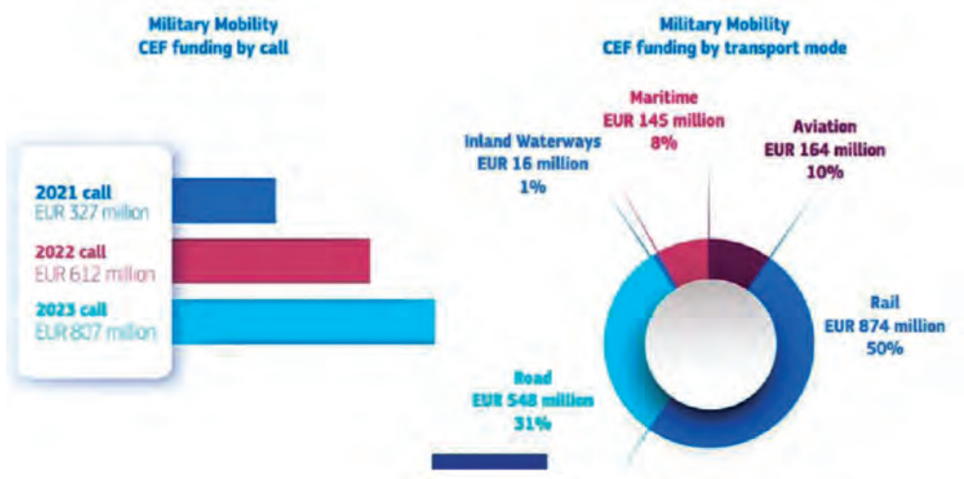


Figure 3. Summary of investments in dual-use infrastructure in Europe between 2021-2023 (Chantraine, 2024)

Figure 4 shows and quantifies how the 21 member states have allocated financial resources to projects aimed at upgrading and developing dual-purpose infrastructures. It can be seen that most states consider the development of railway infrastructure essential, with two thirds of them investing in this sector. Regarding Romania, the investments amount to over 80 million Euros, almost evenly divided between rail and road.

MILITARY MOBILITY IN ROMANIA'S VISION

The Minister of National Defence of Romania signed, on 10 July, during the Washington Summit, the Letter of Intent on the creation of a *Military Mobility Corridor* between Romania, Bulgaria and Greece (RoMoND Press Release no. 152, 2024). This initiative represents an important step in strengthening NATO's defence and deterrence capabilities in the region. At the 2023 NATO Summit in Vilnius, the need to strengthen the deterrence and defence posture through new defence plans

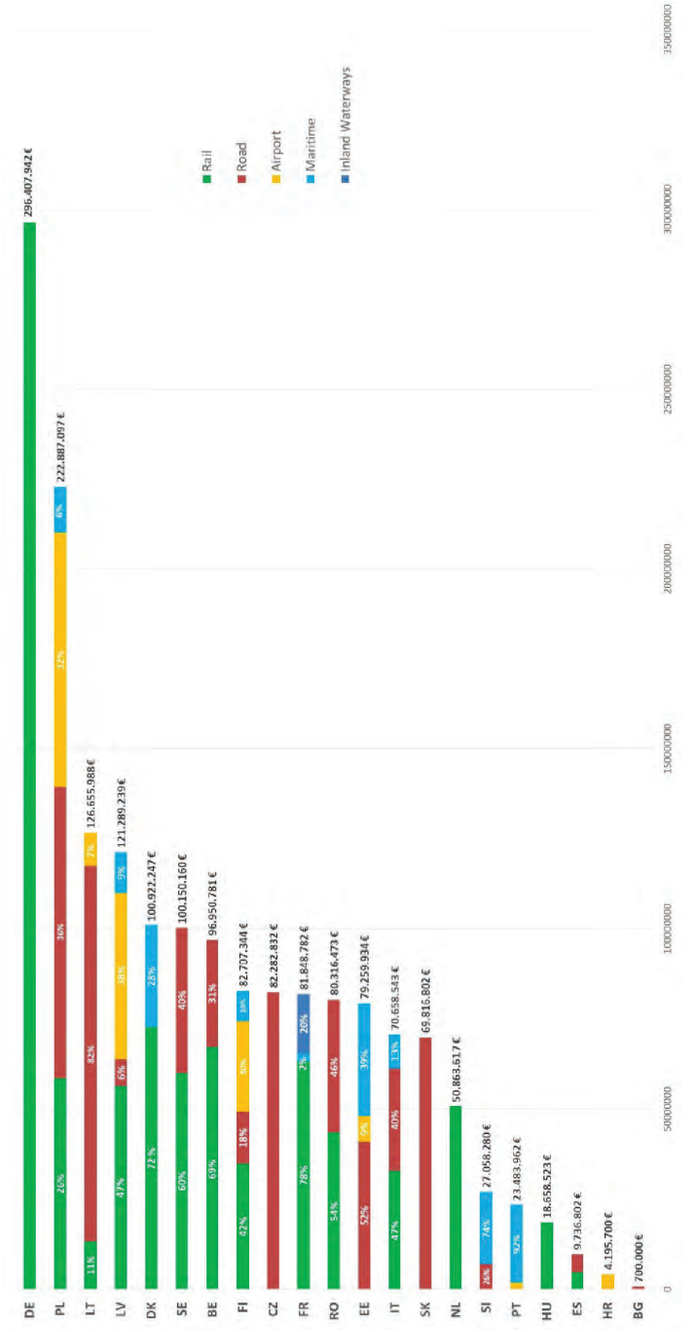


Figure 4: Member states investments in dual-use infrastructure categories assumed in the period 2021-2023 (Ib.)

and accelerate military adaptation was stressed. Adaptation aims to increase forces and equipment and facilitate cross-border transit, including in peacetime.

The letter signed by the three countries is aligned with NATO's objectives of collective defence, rapid reaction and increased interoperability between allies, contributing to a fair distribution of tasks among Alliance members.

The project aims to develop transport corridors (road and rail) between the participating states, reducing bureaucracy in peacetime and optimizing the response in crisis situations, according to NATO and national priorities. The project will benefit from EU initiatives in the field of military mobility, involving coordination between NATO and the EU. Implementation at the national level will require concerted efforts between government institutions.

As shown in *figure 4*, Romania will invest over EUR 80 million in the next period, with 54% of the funds being allocated for the modernization of the railway infrastructure and 46% for the road infrastructure, both falling into the category of dual-utility infrastructures, being beneficial to both the civil and military sectors, if needed.

Another field in which the Romanian Armed Forces have taken important steps with direct effects on military mobility is the procurement of new generation military equipment, which ensures a high level of interoperability in relation to the allies. Of course, in the current security context, the issue of providing the armed forces with high-performance techniques and equipment, at a fast procurement pace and ensuring the country's security interests, represents a real challenge (Nicoară, 2023, p. 74; Hrab, 2022, p. 439). By equipping them with logistics vehicles (IVECO military trucks), armoured personnel carriers (PIRANHA 5, PIRANHA IIIC), tracked infantry fighting vehicles, main battle tanks or light tactical armoured vehicles, the fulfilment of important objectives is envisaged, namely:

improving the transport capacity at the level of the units and subunits of the Land Forces;

- ensuring interoperability with NATO systems;
- increasing operational capabilities by improving the mobility and protection of forces within combat missions and actions;
- modernization of the car fleet, an important element in the gradual development of the potential for logistical support;
- ensuring the manoeuvrability and rapid deployment of forces and means, both within the national territory and in the theatres of operations.

A relevant procurement program in terms of streamlining Romania's military mobility is the procurement of IVECO transport platforms, these vehicles being part of a broader effort to modernize and adapt to the Alliance's standards. IVECO Defence Vehicles offers a range of robust and versatile military vehicles, used for logistics and strategic transport, which comply with NATO requirements in terms of mobility, transport capacity and durability in difficult operating conditions. These transport platforms play an important role in supporting modern military operations, facilitating the rapid movement of troops and equipment across varied terrains, including in multinational operations. The adaptation and integration of these vehicles into the logistical structure of the Romanian Armed Forces contribute to the efficiency and coordination with NATO allies in joint missions and exercises. In addition, the location of the production and maintenance of these vehicles on the national territory is a major advantage for the armed forces in the medium and long run in terms of Romania's defence resources management.

CONCLUSIONS

At NATO and European Union level, a series of measures have been taken in the last decade to contribute to the efficiency of military mobility. As a result of the Russian-Ukrainian conflict, and the lessons learned in terms of actions involving M&T operations, the member states felt the urgent need to accelerate the process of streamlining military transports in the Euro-Atlantic space. In this context, in the period 2021-2023, major projects started, either under the PESCO umbrella or through EDA initiatives, which accumulate an allocated budget of over 1.7 billion Euros, for the modernization and development of infrastructures with dual civil-military applicability. The funded projects aim to develop infrastructures specific to all means of transport, namely by land (road and rail), by air and by water (sea and river).

Equally, NATO organizes regular exercises to test the mobility capacity of its forces. Exercises such as *Saber Guardian* or *Defender Europe* involve rapid movements of troops and related logistics between several states, allowing the testing of logistical corridors and the identification of possible obstacles.

Regarding the perspectives for military mobility in the Euro-Atlantic space, the focus will be on the integration of new technologies, the expansion of logistics networks and the creation of efficient multimodal hubs, which will contribute to increasing the Alliance's defence and rapid reaction capacity. *NetLogHubs*, *Military*

Mobility or *Project Team 'Movement & Transport'* are some of the EDA projects and initiatives, representative in the field of military mobility. At the same time, de-bureaucratization and digitalization are two key elements that will facilitate the fluidization of military transports between member states, by simplifying border crossing procedures, thus leading to much more efficient military mobility.

BIBLIOGRAPHY:

1. Bangală, M.A. (2023). *European military mobility – implications from the perspective of integrated defence resources management*, in *Romanian Military Thinking*, no. 4, pp. 376-395, https://gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20GMR/2023%20gmr/Proceedings%202023/BANGALA.pdf, retrieved on 16 September 2024.
2. Chantraine P. (2024). *Military Mobility Connecting Europe Facility (CEF) & Dual-Use Transport Infrastructure*, *Dual-Use & Military Mobility Seminar*, Ghent, 23 February 2024, https://www.defence-institute.be/wp-content/uploads/2024/03/sem-24-02-23-FEB_Panel-04_Spreker-02_Philippe-Chantraine.pdf, retrieved on 18 September 2024.
3. Chihaia, M.S. (2023). *Advancing military mobility in Europe: An uphill battle*, *Europe in the world programme*, https://www.epc.eu/content/PDF/2023/Military_mobility_PB.pdf, retrieved on 16 September 2024.
4. European Commission (2022). *Action Plan on military mobility 2.0*, https://defence-industry-space.ec.europa.eu/system/files/2022-11/Action%20plan%20on%20military%20mobility%202.0.pdf, retrieved on 13 September 2024.
5. Gheondea, D., Pleșanu, T. (2022). *Military Mobility – A Present-Day Requirement*, in *Romanian Military Thinking*, nr. 1, pp. 42-61, https://gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20GMR/2022%20gmr/2022/GMR%201/GHEONDEA%2C%20PLESANU.pdf, retrieved on 19 September 2024.
6. Hrab, D.E. (2022). *Procurement Programs Challenges for the Sustainability of the Romanian Military Logistics*. Proceedings of the INTERNATIONAL MANAGEMENT CONFERENCE, ASE, Bucharest, vol. 16(1), pp. 439-449.
7. Minculete, Gh., Stan, S.E., Ispas, L., Virca, I., Stanciu, L.&Milandru, M., ... Bădilă, M.I. (2022). *Relational approaches related to digital supply chain management consolidation*. *Sustainability*, 14(17), 10727, https://doi.org/10.3390/su141710727, retrieved on 12 September 2024.
8. Nicoară, G.F., Nicoară, N. (2023). *Challenges of Public Procurement in the Romanian Military System in the Current Security Context*. *AGORA Int'l J. Jurid. Sci.*, 17, 74.
9. Usewicz, T., Czekaj, A., Bartoszek, W. (2022). *Military Mobility: Ambition versus Reality*, in *Safety&Defense*, 8(1), pp. 15-22, https://doi.org/10.37105/sd.173, retrieved on 12 September 2024.
10. Press Release no. 152 din 11.07.2024, Ministry of Defence, https://english.mapn.ro/cpresa/6299_Letter-of-Intent-signed-Romania,-Bulgaria-and-Greece-for-the-creation-of-a-Military-Mobility-Corridor-, retrieved on 12 September 2024.

11. https://cinea.ec.europa.eu/news-events/news/transport-infrastructure-eu-allocates-further-eur-616-million-civilian-defence-dual-use-investments-2022-12-21_en, retrieved on 18 September 2024.
12. https://eda.europa.eu/docs/default-source/eda-factsheets/2018-06-01-factsheet_military-mobility, retrieved on 18 September 2024.
13. https://www.pesco.europa.eu/project/military-mobility/, retrieved on 19 September 2024.
14. https://www.pesco.europa.eu/project/network-of-logistic-hubs-in-europe-and-support-to-operations/, retrieved on 19 September 2024.
15. https://www.dpa.ro/programe-de-inzestrare/, retrieved on 21 September 2024.

COST ARCHITECTURE – FINANCIAL CHALLENGES IN IMPLEMENTING NATIONAL, NATO AND EU SECURITY POLICIES AND STRATEGIES –

Lieutenant Adrian IURA, PhD Candidate
"Lucian Blaga" University, Sibiu, Romania
DOI: 10.55535/RMT.2024.4.45

The paper examines the financial challenges, the possibilities for strengthening the reaction forces and the critical infrastructure that are associated with the implementation of national security policies and concepts, considering Romania's obligations within NATO and the European Union. The main aim of the research is to analyse the impact of budgetary constraints on the state's ability to meet its international security and defence commitments and to respond adequately to emerging risks. The study argues the need for a detailed assessment of procurement decisions in terms of costs and their association with national security, integrating concepts such as "financial security" and "strategic efficiency" to highlight the relationship between economic resources and strategic performance. The methodology adopted includes a qualitative analysis of official documents and financial reports of NATO and EU member states. The results of the research aim to identify sustainable financing solutions capable of supporting national security policies through an optimized allocation of resources.

Keywords: critical infrastructure; European Union; funding; resilience; security;

INTRODUCTION

National security policies and concepts, especially in complex multinational organizations such as the North Atlantic Treaty Organization (NATO) and the European Union (EU), are strongly influenced by their financial architecture. Effective implementation of defence concepts depends not only on political will and military capabilities, but also on the availability and efficient use of financial resources. However, the literature on the financial challenges underpinning these policies remains fragmented and insufficiently explored, especially in terms of the way NATO and the EU manage the tension between national and collective financial commitments. This article aims to address the main gaps in the existing literature by providing an analysis of the cost architecture involved in implementing national security policies in these two major security frameworks.

While numerous studies analyse NATO's burden-sharing model and the EU's Common Security and Defence Policy (CSDP), little research directly compares their financial mechanisms in addressing collective defence needs. The existing literature tends to focus on the political and operational aspects of NATO and EU defence concepts, leaving the financial dimensions under-examined. In addition, there is little comprehensive analysis of the long-term sustainability of defence funding, particularly considering economic downturns, the emergence of new security threats and technological advances. This article fills an existing gap by investigating how financial challenges influence the development, coordination and execution of national security concepts in NATO and the EU.

One contribution this article makes is to comparatively examine the financial approaches in NATO and the EU, providing new insights into how these organizations manage the cost of defence in the context of economic and political constraints. In addition, this study highlights the fiscal inefficiencies resulting from the fragmentation of procurement and defence spending among member states. The article also contributes to the broader discussion on the sustainability of defence funding by addressing emerging threats such as cyber security and space defence, areas that require increased financial attention but remain under-researched.

This article aims to provide a deeper understanding of the theoretical and financial approaches involved in the implementation of national security policies and concepts within NATO and the EU.

METHODOLOGY AND LITERATURE REVIEW

An integrated review of the existing literature and methodological approach used to explore the financial challenges of implementing national security policies in NATO and the EU is provided. It begins by outlining the theoretical framework on the financial architecture of national security, with a focus on the principles of defence economics and cost management. It is followed by a comparative analysis of NATO and EU approaches to security financing, highlighting key differences in their budgetary and financial strategies. The chapter then discusses the main challenges in cost management and defence budgeting, before detailing the methodology used to analyse the financial data. Finally, the chapter identifies gaps in the current literature and suggests directions for future research, laying the groundwork for a more in-depth examination of NATO and EU financial and decision-making structures.

Theoretical framework: The security architecture of financial management

The financial architecture underlying national security policies plays a crucial role in shaping the effectiveness and sustainability of defence concepts. At the heart of this architecture is the interaction between economic resources and military capabilities. The defence economics literature emphasizes the need for nations and international organizations to align their security objectives with their fiscal capabilities. Concepts such as *cost-benefit analysis* and *national security budgeting* are central to understanding how nations allocate resources to defence.

In the context of NATO and the European Union, the challenge is magnified by the collective nature of their defence concepts, which require the coordination of resources across multiple member states. Existing literature, including the work of Hartley (2011) and Sandler and Hartley (1995), illustrates how both organizations grapple with the need to balance the security needs of the group with the individual fiscal realities of their members (Hartley, 2012). This framework is vital to understanding cost-sharing mechanisms and potential inefficiencies that arise in managing collective defence efforts (Sandler, Hartley).

By analysing the financial architecture through the lens of established economic theories, we can better understand how financial constraints influence defence decisions and how different approaches to funding – whether through direct contributions or pooling of resources – influence NATO and EU strategic outcomes.

According to the opinion of specialists, approaches to military equipment procurement are explored through marketing elements, especially customer-consumer relations and sales in the sphere of marketing relations. Therefore,

based on public-private partnerships, financial development could be realized through meeting the needs *"regarding the quality of goods, relationship, service, information and trademark"* (Minculete, Chisega-Negrilă, 2014).

Comparative analysis: NATO and EU approaches to security financing

Both NATO and the EU approach security funding with distinct models, although both share the challenge of coordinating defence contributions from different member states. NATO operates under the principle of burden-sharing, whereby member states are encouraged to contribute 2% of their GDP to defence spending, a goal reaffirmed at several summits, including the 2014 Wales summit and the 2016 Warsaw summit.

The European Union, on the other hand, finances its Common Security and Defence Policy (CSDP) through a combination of national contributions and EU-level funding mechanisms such as the European Defence Fund (EDF). Unlike NATO, which relies heavily on national defence budgets, the EU has taken steps to pool resources at the supranational level, aiming for greater cost efficiency through collective procurement and defence innovation projects.

Despite these differences, both organizations face common challenges related to the sustainability of funding models. Researchers, such as Biscop and J.C. Perry, have highlighted growing concerns about how to sustain long-term defence commitments, particularly in the context of changing political priorities and economic constraints (Perry, Bond, 2012).

Methodological approach: Cost analysis of national security programs

To analyse the financial challenges faced by NATO and the EU in implementing their national security strategies, this study uses a comparative cost analysis methodology. This approach involves the examination of both quantitative and qualitative data on defence spending, cost-sharing arrangements and procurement strategies in the two organizations. The data used in this analysis come from a variety of sources, including official NATO and EU financial reports, national defence budgets, and academic studies on defence economics.

Quantitative data on defence spending, such as the proportion of GDP allocated to defence by member states, are compared between NATO and EU member countries. This comparison makes it possible to identify patterns and discrepancies in the way resources are allocated both within and between the two organizations. In addition, qualitative data from policy documents, speeches and expert interviews are analysed to understand the political and strategic considerations that influence defence spending decisions.

The analysis also considers wider economic factors such as the impact of economic crises on defence budgets and the potential for defence innovation to reduce costs in the long term. By combining these different data sources, the study aims to provide a comprehensive picture of the financial architecture of national security policies in NATO and the EU.

Literature gaps and future research directions

While there is a significant body of literature on defence economics and the financial challenges of collective security, there are still important gaps that need to be addressed. One of these gaps is limited empirical research on the long-term sustainability of defence spending in the face of emerging security challenges such as cybersecurity and space defence. These new areas of warfare require significant investments in technology and infrastructure, but there is no consensus on how these costs should be shared between NATO and EU members.

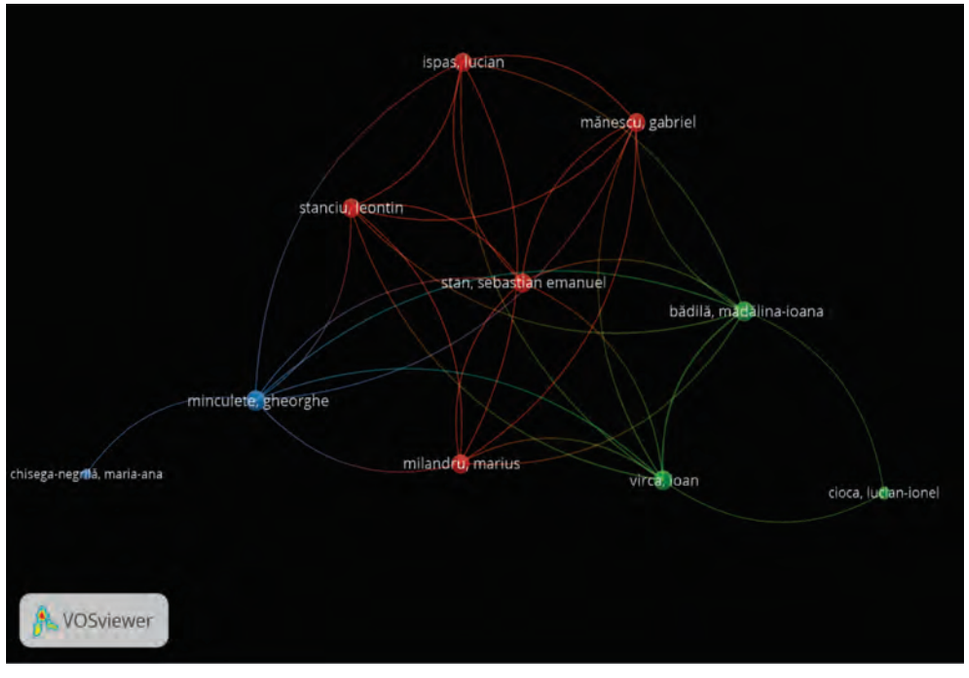


Figure 1: Literature review (author's design)

Another area that requires further exploration is the potential for greater interoperability between NATO and EU defence programs. Although there is considerable overlap between the members of the two organizations, their defence strategies remain largely separate, leading to inefficiencies in resource allocation.

Scholars, such as Fiott, have called for more integrated defence planning (Fiott, 2023), but there is little empirical research on how such integration might be achieved in practice.

Future research should also focus on the impact of defence innovation on cost structures, on how new technologies such as artificial intelligence and autonomous weapon systems will affect the financial architecture of national security. Understanding the costs associated with the development and deployment of these technologies is essential for future defence planning.

NATO AND EU SECURITY CONFIGURATION FOR CRITICAL INFRASTRUCTURE RESILIENCE

Based on the ideology that every country that is part of the North Atlantic Alliance is obliged to withstand a major shock, it must cope in the event of a natural disaster or critical infrastructure failure or military or hybrid conflict.

According to Article 3 of the North Atlantic Treaty, it is stipulated that to *"achieve more effectively the objectives of this Treaty, the Parties, separately and jointly, through continuous and effective self-help and mutual assistance, shall maintain and develop their individual and collective capacity to resist armed attack"* (1949, updated in 2023), which brings the principle of resilience to the forefront.

The principle of resilience can be defined as both a national responsibility and a collective commitment, and each ally must be robust and adaptable to be able to cope with the full spectrum of crises that are envisioned by the alliance. Therefore, resilience relies on strong cooperation between stakeholders (both civilian and military) that can mutually benefit each other in both peacetime and wartime.

Reconfiguration in the operational area – emergence of Battlegroup structures

In view of the operational concept, the agility of alliance forces is *"highlighted by their logistical potential to rapidly combine and move capabilities over long distances to conduct planned operations in austere, fragile environments with vulnerable critical infrastructure"* (Minculete, 2023, p. 82). In this context, it may be noted that in the sphere of the North Atlantic Alliance, the defence planning process is established in detail and should also be taken into account by the member countries in order to identify risks and build specific resilience through which both national and multinational resources can be committed (NATO, 2017, pp. 3-5).

Given the role played by operational logistics and the financial sphere, its range of importance and action is intended to encompass both the national area

of a member state and the multinational area, given the partnerships between powerful countries, which have formed Battlegroups (BGs) following troop deployments.

Therefore, within Romania, a highly responsive French battalion was deployed as a framework nation.

Table 1: French-led Battle Group in Romania (BGFP) (author's design)

Contributor	Number of militaries involved	Types of Forces involved
France	550	1 x Infantry Battalion
Belgium	248	Combined Arms Battle Group
Poland	230	1 x Mechanized Company
United States of America	120	Cavalry unit
A total of approximately 1,150 military		

Since the outbreak of the armed conflict in Ukraine, NATO has been able to deploy many troops in the Eastern flank to secure and strengthen its defence, considering the development of the war in Eastern Europe. As shown in *figure 2*,



Figure 2: Deployment of NATO forces on the Eastern Flank (NATO, 2017, ib.)

the multinational structures of the North Atlantic Alliance have started to deploy more and more forces around the Eastern flank to be able to support and at the same time maintain security and defence in case of a possible attack by Russia or a possible defeat of Ukraine.

Improving the financing of security, defence and military logistics based on the Ukrainian model

Based on the concept of transforming alliance functionality, operational logistics is a system of systems, capable of anticipating and solving the requirements of the forces on which the tactical situation will depend. The requirements in support of operational or joint logistics have led to a much higher level of understanding of this field, following the experiences of the campaigns in Afghanistan and Iraq (McDermott, 2013, pp. 16, 32).

The armed conflict in Eastern Europe has forced the member states of NATO and the European Union to carry out the necessary structural and functional reorganizations to increase the resilience of their armed forces.

Therefore, from the point of view of economic, social and military stability, the North Atlantic Alliance has imposed and applied the necessary measures to increase combat power, forcing the modernization of strategic, joint (operational) and tactical logistics, and the rate of the effect of increasing the performance of modernization of security and defence from the financial point of view can be represented by the following econometric relationship (adapted from Minculete, 2023, p. 110):

$$\% Rcr = [(Mo * Lm/Ln) - Cv] *100,$$

of which the following data are expressed according to the following legend:

- % Rcr = representing the rate of performance growth;
- M = the mission the logistics must fulfil;
- Lm = modernized logistics, able to cope with any type of disaster (with increased resilience);
- Ln = non-modernized logistics, which could cope for the full capabilities;
- Cv = the value of the consequences of the manifestation of risk factors.

Given the adaptation of the econometric relationship of the performance growth rate econometric relation, represented above, and based on *figure 2*, it is exploited the main role through which a nation has to go through a modernization process. The notions in the figure are based on the determinations and structural changes that Ukraine has made to reach the performance developed in the type of the Russian-Ukrainian conflict.

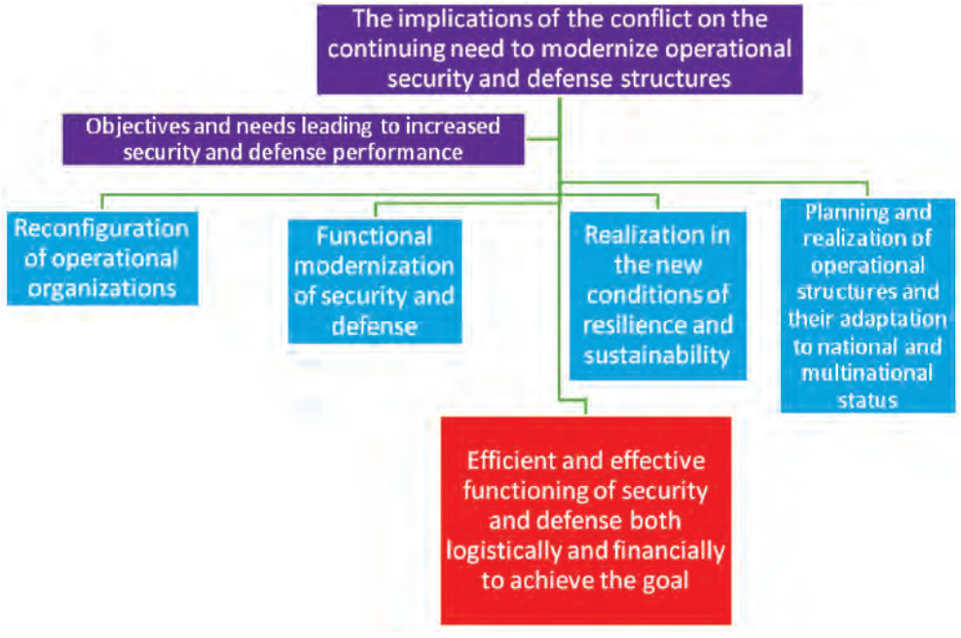


Figure 3: Functional determinations to achieve optimal performance and the goal
(author's compilation)

Therefore, it can be concluded that the need to set and achieve an objective on the operationalization of combat forces in the conditions of the 21st century (uncertainty and high-risk) can determine the overall performance that is found in operational structures that have led to adequate growth in the structural spheres.

THE INFLUENCES OF FINANCIAL MANAGEMENT AND MATHEMATICAL RELATIONSHIPS IN DECISION-MAKING FOR SECURITY AND DEFENCE AT NATIONAL, NATO AND EU LEVEL

In the complex web of national, NATO and EU security and defence decision-making, the interplay between financial management and mathematical relationships has a profound influence, and this chapter will delve into the complex dynamics where fiscal strategies and quantitative analysis intersect, shaping policies and strategies crucial to protecting interests and ensuring security and defence.

The mathematical relationships that make it possible to strengthen logistical and financial management

Based on the idea that today's economic requirements have evolved, it is appreciated that supply chain management of operational structures needs smart digital technologies. The article emphasizes the ideologies of variety, volatility,

social, economic and geopolitical conflict issues, which, through the relevance of supply chain management (SCM), become essential in the functional stages of the concepts *"Society 5.0"* and *"Industry 5.0"* (Minculete, 2021).

Therefore, by adapting the econometric relations of probabilities, decision and occurrence factors, and the optimal determinant of expectations, their applicability in the military environment will be observed, which is aimed at increasing the level of financial and logistic performance effects, from a structural and functional point of view (Minculete et al., 2022).

In a short exercise, the probability of occurrence of the event *"c"* (costs), lead to the increase in the functional performance in the SCM through the following variables: Cr and Cm, the probability of occurrence of the event *"i"* will express the adaptation of each decision node, related to each decision variant at the level of the operational structure (EmDi), realizing an evaluation of the specific costs of each purchase, installation and functional checks of equipment and systems. Therefore, the relationship formula of the decision determinant and the optimal expectation determinant is given by the following econometric formulae:

$$V_{op} = \max E_m i, \text{ where } E_m i = \sum_{i=1}^{m} Pc * Ric$$

- Pc = represents the probability of event *"c"* occurring;
- Ric = represented by the variable *"i"* influenced by event *"c"*;
- Emi = represents the expectation determinant of the decision node;
- Vop = is the Optimal Decision Variant, where there is the highest mathematical expectation and from a value and decision point of view, it represents the optimal decision.

Therefore, the adaptation to the strategic miliary model complements the risk management with the following statement: *"according to the specific implementation method, the construction of the decision tree is based on the three decision variants (V1 - V3); the risk nodes (R1 - R3); the decision nodes (D1 - D9); the terminal nodes (E1 - E18)"* (Ib.).

Following the fictitious construction of the decision tree, the following will be presented:

- V1 - V3 are the decision alternatives;
- R1 - R3 are the risk nodes (risk management);
- D1 - D9 represent the decision nodes, where the optimal decision will be made by means of decision management out of the total of the 3 variants;
- E1 - E18 are the final nodes, from which the acquisition costs are derived, in other words Ei is represented by the possibilities.

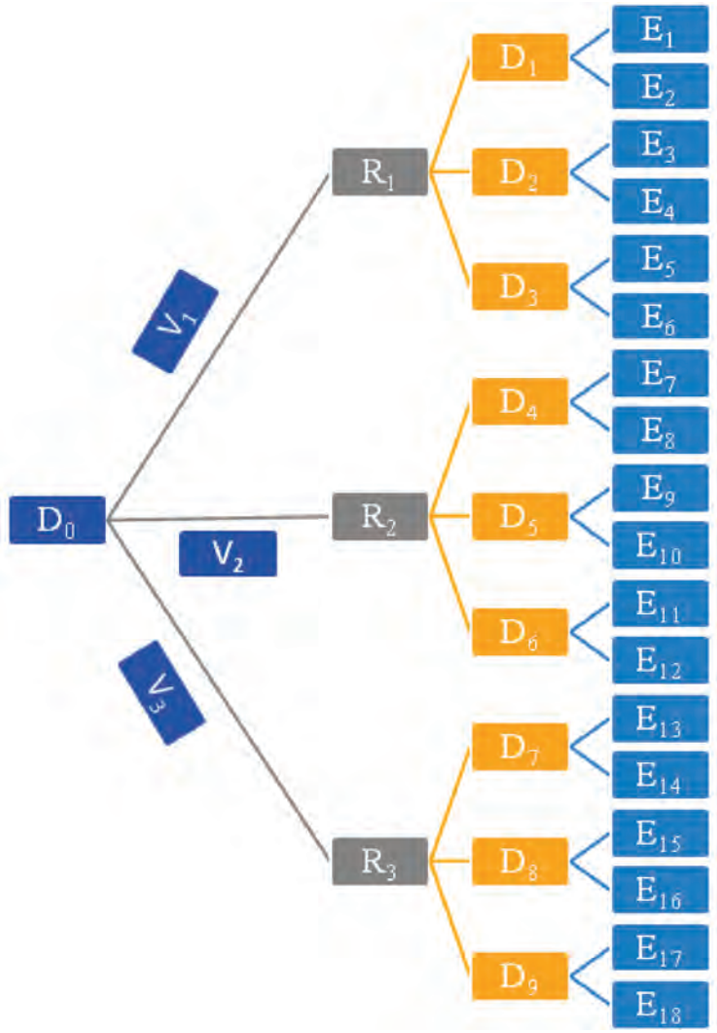


Figure 4: Results of the decision tree according to the situation created (author's compilation)

Therefore, based on the above scheme, it can be concluded that the operational type of structure can be based on these types of relationships and mainly on the decision tree to make the optimal decision, from a financial point of view.

Direct financing of security and defence at the level of the North Atlantic Alliance

Starting from the idea that every country has a budget and an annual program for the purchase of military equipment to maintain national security and defence, it can be said that in both NATO and the European Union there is the same method,

namely the existence of a budget. This budget is at the basis of the North Atlantic Treaty ideology in relation to the possibility of mutual support and collaboration, both in terms of financial resources and in terms of the conduct of military operations and missions, but at the same time this common budget is also designed to help build an essential military infrastructure.

The common funding modality used by NATO is of a pooled funding type, and the shaping of such a budget is based on both the accumulated contributions from each ally and the following forms:

- Trust Funds;
- In-kind contributions;
- Ad hoc sharing arrangements;
- Donations.

The principle of joint financing

Since the conclusion of the North Atlantic Treaty in 1949, pooled funding has been at the heart of the Alliance's strategy to maintain consistent support for its objectives, priorities and tasks. The principle of this funding is that allies *"pool"* a portion of their financial resources to provide support for defence programs and capabilities.

The joint funding commitments will apply to both military and civilian budgets, but also within the sphere of influence of the NATO Security Investment Program (NSIP). Therefore, the way to calculate the share of financial resources that are pooled in a common budget is the relationship of the total agreed costs divided by the Gross Domestic Product of each member country. The formula for the relationship is as follows:

- Cfca = Tc/Vnb, of which the legend of the variables is as follows:
- C_{fr} = Resource Sharing Quota;
- T_c = Total costs;
- V_{nb} = Gross Domestic Product.

Following the principle and the joint funding, participating countries are obliged to identify funding priorities, while NATO has the role of ensuring political security. Jointly funded programs are therefore composed according to the number of countries involved, joint funding arrangements and management structures. The most recent funding initiative is the Defence Innovation Accelerator for the North Atlantic (DIANA) (NATO, 2024).

COMPARATIVE ANALYSIS: NATO VS. EU FINANCIAL APPROACHES

The financial mechanisms supporting national security policies in NATO and the EU are shaped by distinct organizational frameworks, political imperatives and historical legacies. However, both face common challenges in ensuring the allocation of sufficient resources to meet defence and security objectives. This chapter provides a comparative analysis of how NATO and the EU structure their defence spending, manage acquisition costs, address fiscal imbalances, and cope with the financial impact of economic crises on security financing. By exploring the similarities and differences in their financial approaches, this chapter highlights the challenges these organizations face in maintaining effective and sustainable defence capabilities.

Budget allocation and defence spending

One of the most significant differences between NATO and the EU is how each organization allocates its defence budget. NATO, as a military alliance, relies primarily on the national defence budgets of its member states, with a widely accepted benchmark of allocating 2% of GDP to defence spending. In practice, however, only a limited number of NATO member states consistently meet this target, leading to uneven burden-sharing. The United States of America, for example, has historically contributed a larger share of NATO's defence budget, leading to tensions with the European allies that fail to meet the spending threshold. This disparity in defence spending creates both political and operational challenges within NATO, as the alliance is heavily dependent on the financial contributions of a few key members.

Instead, the EU uses a dual financial structure for its defence initiatives. National defence budgets remain under the control of individual member states, but the EU has introduced collective funding mechanisms, such as the European Defence Fund (EDF) and the Permanent Structured Cooperation (PESCO). These initiatives are designed to pool resources, rationalize procurement and strengthen defence cooperation between EU member states. However, these collective mechanisms represent a step towards reducing the fragmentation of European defence spending, while the overall impact remains limited by the modest size of EU defence budgets compared to NATO contributions at national level. The Union's defence spending is constrained by competing priorities across the broad budgetary spectrum, including economic, social and environmental objectives.

Cost management: Procurement and innovation

Within NATO, procurement is largely decentralized, with each member state responsible for acquiring military equipment and technology. It leads to duplication of effort, as each country procures similar equipment independently, often resulting in inefficiencies and higher costs. In recent years, NATO has attempted to address this problem through initiatives aimed at increasing interoperability and joint procurement (Smith et al., 2020). However, the lack of a centralized procurement process continues to limit the organization's ability to achieve cost reductions and economies of scale.

The European Union has created some significant programs in collective purchasing namely EDF and PESCO. These initiatives are designed to encourage member states to collaborate on defence projects, reducing duplication of effort and increasing cost efficiency. For example, PESCO promotes the joint development of military capabilities by allowing member states to share research, development and procurement costs. Despite these efforts, the EU faces its own set of challenges, including bureaucratic delays, competing national interests and the relatively small scale of its defence projects compared to NATO's.

In terms of defence innovation, both NATO and the EU are investing in new technologies such as cyber defence, artificial intelligence and autonomous systems (Wrona et al., n.d.). However, the pace of technological progress poses a financial challenge for both organizations, which must balance the need to invest in state-of-the-art capabilities with the reality of constrained defence budgets. While NATO benefits from substantial defence investments from the United States of America, EU defence innovation efforts are more constrained by limited financial resources and a slower and more fragmented decision-making process.

Fiscal imbalances and the impact of economic crises on security financing

Fiscal imbalances and economic crises pose significant challenges to the financial stability of both NATO and the EU, affecting their ability to effectively implement security policies. These imbalances, driven by the unequal contributions of member states and the different economic capabilities of each nation, create long-lasting tensions within both organizations. In addition, economic crises – such as the 2008 financial recession or the recent COVID-19 pandemic – intensify these problems, forcing nations to prioritize domestic economic recovery at the expense of defence spending. This section examines how these fiscal imbalances and economic crises affect the financial structure and defence capabilities of NATO and the EU.

Fiscal imbalances: National versus collective interests

Within NATO, the burden-sharing debate highlights the disparity between member states, with wealthier nations such as the United States of America consistently meeting defence spending benchmarks while many European allies fail to do so. It creates political tensions and uneven financial burdens within the Alliance. In the EU, fiscal imbalances stem from the conflict between national sovereignty and collective security, leading to a fragmented defence market. Smaller member states facing financial constraints struggle to contribute effectively, further weakening common defence initiatives.

The impact of crises on security and the need for sustainable funding models

It is examined the impact of economic crises on defence funding in NATO and the EU, highlighting how recessions such as the 2008 financial crisis and the COVID-19 pandemic have led to significant cuts in military budgets. These cuts have undermined collective security efforts, delayed modernization programs and weakened operational readiness. Both organizations have struggled to maintain their defence capabilities, with governments prioritizing domestic economic recovery. Fiscal pressures have deepened imbalances between member states and the long-term sustainability of NATO and EU defence initiatives.

To mitigate the negative impact of fiscal imbalances and economic crises on security financing, both NATO and the EU need to adopt more flexible and sustainable financial strategies. NATO could improve its cost-sharing mechanisms, encouraging more equitable contributions from member states, while the EU could accelerate its efforts towards collective procurement and pooling of resources. In addition, both organizations need to develop contingency financial plans to ensure that defence funding remains resilient during economic downturns, possibly through the creation of emergency defence funds or long-term financial frameworks to protect defence budgets from external shocks.

Comparative study results

The study shows that fiscal imbalances within NATO and the EU have a significant impact on their ability to implement effective national security policies. Within NATO, the current burden-sharing issue remains unresolved, with a persistent dependence on a few key contributors, notably the United States of America, to meet the organization's defence requirements. Despite political pressure to reach the 2% of GDP spending target, many European members continue to fall short, leading to an uneven distribution of defence resources. This disparity creates political friction,

but it also weakens NATO's collective defence posture, underscoring the need for new funding mechanisms that consider the financial realities of member states while maintaining the Alliance's security objectives.

In the EU, the results show that the fragmentation of the defence market and the tension between national sovereignty and collective security hinder the development of an effective and unified defence strategy. Although initiatives such as the European Defence Fund (EDF) and Permanent Structured Cooperation (PESCO) have been designed to promote joint projects and rationalize defence spending, they have not yet reached their full potential. The reluctance of EU member states to pool their resources and transform defence capabilities into ongoing collaboration can limit the effectiveness of programs. This fragmentation often leads to inefficiencies and duplication in defence spending, hampering EU efforts to develop a stronger and more coherent defence policy.

Finally, the article highlights the long-term impact of economic crises on defence funding and preparedness in both organizations. Economic downturns, such as the 2008 financial crisis and the COVID-19 pandemic, have led to significant cuts in defence budgets as governments prioritize domestic recovery efforts. These cuts in defence spending have led to delayed modernization programs, diminished military capabilities and decreased operational readiness. The results of the approaches, indicate that both NATO and the EU need to build more resilient financial models that can sustain defence funding in times of economic stress, ensuring that national security policies are not undermined by external economic challenges. Overall, the study's findings underline the importance of adopting sustainable and adaptable financial strategies to maintain and enhance collective security within NATO and the EU.

CONCLUSIONS

The implications of this study underline the need for both NATO and the EU to rethink their financial structures for the implementation of national security policies, particularly in view of growing fiscal imbalances and the impact of economic crises on defence budgets. The main beneficiaries of these findings are policymakers and defence planners. By understanding the burden-sharing challenges and pressures on defence budgets in relation to economic downturns, policymakers can develop more resilient financial designs. This research also offers useful data to financial analysts and researchers by providing a comprehensive view of the cost architecture behind collective security efforts as well as insights into more sustainable defence funding models.

The added value of this paper lies in its in-depth analysis of fiscal imbalances, burden-sharing challenges and the implications of economic crises, all of which are explored in both NATO and EU contexts. While previous studies have often focused on isolated aspects such as political or institutional factors, this research integrates the financial dimensions, providing a broader understanding of the interlinked issues. Moreover, it introduces the concept of *resilient defence financing* in the face of economic crises, a timely and under-explored area in the existing literature, particularly considering recent events.

However, this study has certain limitations. While it provides a comprehensive overview, the analysis is constrained by the lack of access to classified financial data, focusing on larger member states, which may underestimate the contributions and challenges of smaller countries. In addition, the dynamic nature of global economic conditions may change the relevance of the findings over time, requiring further research to account for future developments. Comparisons with previous studies show that, while much has been written on the political and institutional challenges, the focus of this article is on the financial architecture that adds a critical dimension to the current discourse on collective security within NATO and the EU.

BIBLIOGRAPHY:

1. Fiott, D. (2023). *In every crisis an opportunity? European Union integration in defence and the War on Ukraine*. In *Journal of European Integration*, 45(3), pp. 447-462. https://doi.org/10.1080/07036337.2023.2183395, retrieved on 12 August 2024.
2. Hartley, K. (2012). *Conflict and Defence Output: An Economic Perspective*. In *Revue d'économie politique*, vol. 122(2), pp. 171-195, https://doi.org/10.3917/redp.218.0171, retrieved on 22 July 2024.
3. McDermott, R.N. (2013). *Russia's strategic mobility – Supporting "hard" power to 2020?* Sweden: Stockholm. The Swedish Defense Research Agency.
4. Minculete, Gh. (2021). *Conceptual Approaches of Industry 5.0. Correlative Elements with Supply Chain Management 5.0*. 22(5).
5. Minculete, Gh. (2023). *Determinări relaționale privind modernizarea logisticii operaționale*. Sibiu: Editura Techno Media.
6. Minculete, Gh., Chisega-Negrilă, M.-A. (2014). *Marketing Management Relational Approaches Focused on Consumer's and Customer's Needs and Desires*. 17(2).
7. Minculete, Gh., Stan, S.E., Ispas, L., Virca, I., Stanciu, L.&Milandru, M., Mănescu, G., Bădilă, M.-I. (2022). *Relational Approaches Related to Digital Supply Chain Management Consolidation*. *Sustainability*, 14(17), 10727, https://doi.org/10.3390/su141710727, retrieved on 22 May 2024.
8. Perry, J.C., Bond, M. (2012). *Change in Defense Mechanisms During Long-Term Dynamic Psychotherapy and Five-Year Outcome*. In *American Journal of Psychiatry*, 169(9), pp. 916-925, https://doi.org/10.1176/appi.ajp.2012.11091403, retrieved on 12 August 2024.

9. Sandler, T., Hartley, K. (2007). *Chapter 20 Defense in a Globalized World: An Introduction*. In *Handbook of Defense Economics*, vol. 2, pp. 607-621). Elsevier, https://doi.org/10.1016/S1574-0013(06)02020-5, retrieved on 12 August 2024.
10. Smith, S.J., Gebhard, C., Graeger, N. (2020). *EU-NATO Relations: Running on the Fumes of Informed Deconfliction* (1 ed.). Routledge, https://doi.org/10.4324/9780429454462, retrieved on 22 May 2024.
11. Wrona, K., Moye, T., Lagadec, P., Street, M., Lenk, P.&Jordan, F. (n.d.). *Cybersecurity Innovation in NATO: Lessons Learned and Recommendations*.
12. NATO TOPICS, https://www.nato.int/cps/en/natolive/official_texts_17120.htm, retrieved on 30 August 2024.
13. NATO (2017). NATO Headquarters Supreme Allied Command Transformation, Transforming NATO Logistics and Sustainability Today and into the Foreseeable Future: *A NATO Food-for-Thought Paper*, USA: Norfolk, Virginia, pp. 3-5.
14. North Atlantic Treaty (4 April 1949, updated on 19 October 2023), https://www.nato.int/cps/en/natolive/official_texts_17120.htm, retrieved on 22 May 2024.
15. NATO (2024). *Funding NATO*, https://www.nato.int/cps/en/natohq/topics_67655.htm#management, retrieved on 22 May 2024.
16. PESCO, https://www.pesco.europa.eu/about/, retrieved on 22 May 2024.

BLUEPRINTS FOR CHANGE – BENCHMARKING GENDER DYNAMICS WITHIN NATO AND EU –

Major Silvia STANCIU, PhD
Ministry of National Defence
DOI: 10.55535/RMT.2024.4.46

Russia's full-scale invasion of Ukraine has regionally and globally shifted the security paradigm and consequently undermined the international peace and stability. In this context, global security organizations have been put to a hard test and determined to use the blueprints of deterrence and defence based on political-military cohesion, resilience and adaptation. Developments on all dimensions of the defence and security sector have been reconsidered, thus the gender perspective being reconfirmed as crucial on the agendas of NATO and EU across all core tasks. Military capability, effectiveness and interoperability represent the most valuable assets for the challenging security landscape unfolding at present, therefore benchmarking the NATO and EU gender developments is key in the process of advancing gender equality and enhancing its integration in a coherent and coordinated manner. The new adopted Women, Peace and Security policies, plans and procedures enable both NATO and the EU to respond better to the broader security challenges and to thoroughly approach the intersection between gender and all other emerging security threats, by recognizing and employing diversity as a catalyst for a more secure future.

Keywords: Ukraine; shift mechanisms; gender dynamics; integration; diversity;

INTRODUCTION

The continuously evolving and changing security environment has brought to the forefront of international security-providing organizations the ongoing need to augment the two coordinates of deterrence and defence, relying in this endeavour on political cohesion, resilience, and military adaptation. The war in Ukraine, the conflict in the Gaza Strip, terrorist threats, as well as the visibly assertive attitude of China under Xi Jinping's leadership (Loh, 2024, p. 7), overlaid by a wide range of security challenges associated with elements such as demography, climate, resources, or public health, which are also in full evolution, are the reason why the gender perspective has continued to be validated as crucial on the NATO and EU agendas in all core tasks. The adoption of the updated version of the *Alliance's Policy on Women, Peace, and Security* at the NATO Summit in Washington demonstrates, on the one hand, the firm commitment to integrating gender perspectives into activities and across all specific NATO structures (Washington Summit Declaration, 2024, point 35) and, on the other hand, the profound understanding of the interconnection between advancing the gender agenda and improving the Alliance's ability to understand conflict-generating factors and operating environments, identify security risks and vulnerabilities, develop more tailored and gender-sensitive interventions, and identify effective solutions (NATO Policy on Women, Peace and Security, 2024, point 19). The conflict in Ukraine, generated by Russia's unprecedented aggression, has brought to the dialogue on ensuring peace and security in the Euro-Atlantic area the critically important idea that, in an interconnected world, isolationism will not provide safety to any state. The current security challenges are far too great, and the competition is too fierce for any nation or even security organization to combat them alone. Therefore, the only winning option for them lies in partnerships and cooperation, especially if they leverage resources and geography. In this context, we observe that the European Union approaches gender as a facilitator of interoperability and supports its members and partners in developing security and defence institutions that are accessible and responsive to the needs of both women and men, while also concretely promoting the participation and representation of women at all levels of national armed forces. The gender dynamics within NATO and the EU are in continuous flux thanks to the deliberate choices of the members and partners of the two organizations, as well

as the political will to thoroughly address the intersection between gender and all other emerging security threats, by recognizing and utilizing diversity as a catalyst for a safer future. This study further aims to adopt a nuanced and comparative approach to the integration of the gender concept within NATO and the EU, while exploring in parallel the policies, plans, and implementation of gender in current military operations.

GENDER DYNAMICS WITHIN NATO

As NATO advances in a complex geopolitical context, deterrence and defence are becoming increasingly important. Without a doubt, Russia's aggression against Ukraine has provided a powerful reminder that we must expect the unexpected and, equally, we must be prepared for all types of scenarios that may unfold in the future. Under these circumstances, it is essential to maintain conventional fighting forces, as it paradoxically constitutes a premise for dialogue, while developing the ability to combat unconventional threats and introduce new technologies with the necessary skills for their effective use. Therefore, it is important to encourage diversity within the workforce, particularly in the military, to generate the skill sets and mindsets necessary to counter the conventional and unconventional challenges we face.

Developments and Key Milestones regarding Changes to Gender-Related Policies, Strategies, and Action Plans at the North Atlantic Alliance Level

With the occasion of NATO's 75th anniversary and nearly 25 years since the adoption of UNSCR 1325 by the UN Security Council, the world is facing the highest number of violent conflicts since the Second World War. Millions of women worldwide are thus experiencing a regression of their overall rights, along with a shrinking access to participation in security efforts and peace negotiations, disproportionately affected by ongoing conflicts. Currently, NATO is navigating the Euro-Atlantic area, dealing with the turmoil created on multiple fronts by the conflict in Ukraine, and through the mechanisms of change adopted in both theoretical and legislative terms, it demonstrates its intention to remain a presence firmly anchored in protecting and building upon the achievements already made in advancing the Women, Peace, and Security agenda.

Building on this reality and aligning with the 2022 Strategic Concept, NATO's new gender policy provides the necessary political framework for the Alliance to continue promoting the UNSCR 1325 agenda. The document acknowledges that the integration of the gender dimension enhances NATO's political decision-making

processes, operational effectiveness, and all efforts to achieve gender equality. It also recognizes that gender equality and the Women, Peace, and Security agenda are integral to sustainable peace and reflect the core values and priorities of the Alliance.

Thus, the new policy outlines the relevance and status of the Alliance, presenting essentially four strategic objectives:

1. *Strengthening gender-responsive leadership and accountability processes in this area;*
2. *Increasing women's participation at all levels of activity, including decision-making and leadership roles;*
3. *Preventing threats that disproportionately affect women and girls;*
4. *Protecting women and girls from gender-based violence.*

The four strategic objectives mentioned above are inspired by the global gender agenda, adapted to the Alliance's mandate and mission, with the aim of guiding NATO's present and future political and military efforts, both internally and externally.

As a new element, looking beyond the lines that define traditional security threats, the Policy brings to the forefront the interconnection within NATO between the gender agenda and the human security agenda, particularly in the sphere of sexual violence in armed conflicts, a fact also observed in the evolution of the conflict in Ukraine. Thus, we observe that the two agendas reflect people-centred, human rights-based approaches that complement and reinforce each other, even though they remain separate in essence. While the concept of human security considers the safety and security of all people, the concept addressed through UNSCR 1325 emphasizes the impact of gender in armed conflicts, an impact that is often disproportionate due to gender inequality and discrimination. Sexual violence in armed conflicts, used as a deliberate war tactic, represents an acute threat, as it undermines societal resilience and regional stability on multiple critical fronts (NATO Policy on Women, Peace and Security, 2024, point 6). For this reason, through the new Gender Policy, NATO is committed to ensuring the effective prevention and response to this threat in all missions, operations and activities conducted under NATO's aegis, thus aligning with the NATO Policy on Preventing and Responding to Conflict-Related Sexual Violence (CRSV, 2021) as well as with NATO's Women, Peace, and Security Action Plan for the 2021–2025 period.

The gender perspective is key to understanding current conflicts, especially now, when they are fought both on the battlefield and beyond, in the areas of economic sanctions, hybrid warfare and disinformation. In this regard, the Gender Policy

adopted in 2024 refers for the first time to new aspects associated with emerging security challenges, such as gendered disinformation, gender-based violence facilitated through technology, the gender dimension of climate change, and the use of artificial intelligence in everyday life. It also emphasizes the importance of partnerships with civil society and advocates for closer cooperation with the private sector, particularly concerning technology-related threats.

In an organization like NATO, which is based on the respect for shared values, the gender perspective can be deliberately leveraged to enhance any doubts regarding whether Western international organizations are defending their own interests at the expense of the democratic values upon which they were founded. Therefore, if the gender perspective is not accepted as an essential premise in negotiating, achieving, and guaranteeing peace, NATO risks its reputation as a security-providing organization due to the use of disinformation tactics in this dimension, the insertion of cognitive biases in information analysis, the reduction of resilience towards its own societies, or by diminishing the effectiveness of planning and conducting operations (Military Voices on the Gender Perspective: A NATO Anthology, 2024, p. 8).

Recognized within NATO's Warfighting Capstone Concept, technology serves as a critical facilitator in the development of military capabilities. At the same time, the gender perspective needs to be considered to maximize the advantages created through the use of military technologies, as incorporating gender differences as part of the implementation process of gender in specific capability requirements can ensure that armed forces are better trained and prepared to respond to any future threats. NATO utilizes innovative and disruptive technologies as part of its deterrence and defence posture. Therefore, if technological capabilities are developed with a gender-sensitive approach, all future fighters are likely to be able to use advanced technological systems and capabilities that enhance effectiveness, protection, and connectivity on the battlefield, within the context of responsibly designing equitable technologies guided by a human rights-centred approach and the integration of the gender perspective. The new benchmark is based on ongoing military adaptation efforts, including the complete and rapid implementation and operationalization of two high-level military concepts: the *Concept for the Deterrence and Defence of the Euro-Atlantic Area*, which focuses on the engagement of force for deterrence and defence in the present, and the *NATO Warfighting Capstone Concept*, which provides a 20-year vision for the development of the Alliance's military power and establishes a practical path to turn this vision into reality (Bâtcă, 2023). In this regard, the Alliance responds to current challenges in the security environment

by strengthening advanced conventional capabilities, investing in new platforms, and adapting its exercises, information environment, and air and missile defence posture (Ministry of Foreign Affairs, Romania in NATO, 2024), as well as by utilizing diverse mechanisms, such as the gender agenda, which facilitates a comprehensive understanding of the international security environment as a whole. Thus, in fulfilling deterrence and defence objectives, gender plays an essential role in the development of the Alliance's areas of action, providing granularity (NATO Policy on Women, Peace and Security, 2024, point 20) and ensuring robust forces whose training is tailored to the complexity of the operational environment (Ib., point 24). In the area of crisis prevention and management, NATO Allies show increased interest in integrating the gender perspective as it contributes to refining the information management process, operational leadership, and decision-making at the Allied level, within a political and military context. Moreover, the gender agenda, through its relevance and characteristic diversity, easily ensures effective and nuanced prevention and response to crises through implementation mechanisms (Ib., point 26). The objective of ensuring security through cooperation strengthens the Alliance and secures the safety of millions of European citizens while also contributing to the preservation of peace and stability in the Euro-Atlantic space. The gender perspective contributes in this context to facilitating political dialogue and deepening practical cooperation with partners, cooperation based on a shared value vision, respect, and mutual benefits. At the NATO level, the extensive network of relationships and partnerships essential for protecting common goods globally, enhancing resilience, and maintaining a rules-based international order provides the right framework for advancing the international gender agenda, focusing relevant actors on implementing UNSCR 1325 and the decisive means to achieve the objectives of NATO's gender policy on a large scale.

In another context, the gender perspective is also an opportunity, representing a means of building and ensuring the connection between political ideals and military operational necessity. Through a better understanding of the gender perspective, NATO can comprehensively address the vectors of threat and existing vulnerabilities within the societies it seeks to protect. Women communicate effectively, build relationships, and manage complex social dynamics differently and complementarily to men, and their skills can be invaluable for engaging local populations, gathering intelligence and supporting mission success in conflict zones. Therefore, the assertion brought into discussion is clear: when women participate in shaping security strategies, their unique perspectives lead to the identification and selection of more comprehensive and sustainable solutions regarding this dimension.

During global security challenges, the world witnesses the profound impact of women's active participation in the actions carried out by the Armed Forces. Ukraine is a testament to this reality, with 66,000 courageous women serving their country in uniform, over 5,000 of whom are on the front lines, demonstrating resilience and courage in the face of Russian aggression (Military Voices on the Gender Perspective: A NATO Anthology, 2024, p. 18). Their indispensable role underscores the universal need for the integration of gender into security sectors worldwide, and their example illustrates a path toward building a more inclusive and resilient security landscape, where every individual, regardless of gender, can significantly contribute to global peace and stability.

Reflections and Perspectives

Integrating the gender perspective is and will continue to be an integral part of NATO's efforts to ensure peace, stability and security, contributing to strengthening unity, legitimacy, resilience and cognitive superiority. Thus, in the future, NATO forces will remain more accountable for their actions, opting to operate exclusively within the legal framework adopted by the Alliance, upholding the highest standards of behaviour and committing to ensuring that the military actions in which they participate – be they exercises, operations or responses to natural disasters – will have a minimal impact, as short-term as possible, on the entire population.

NATO must also develop a workforce with the right proportions and the appropriate diversity of talents to have the real capacity for deterrence and defence in the context of a potential future war. It certainly entails that the Alliance will ensure that both women and men have equal access to the security sector and the armed forces, and therefore they can have the opportunity to defend their fundamental values, namely freedom, peace and security.

Finally, NATO must develop the appropriate processes and capabilities to conduct future warfare by integrating a gender perspective. The Alliance, during its multi-domain operations supported by new technologies, should collect sex- and age-disaggregated data as a strategic advantage. Such data can effectively facilitate gender analyses of personnel functions, thereby enhancing situational awareness on the battlefield and understanding the human environment operating within it. These actions will document the decision-making and planning processes, increasing the efficiency of NATO's future military operations and activities, and thereby contributing concretely to ensuring mission success.

GENDER DYNAMICS WITHIN THE EU

The European Union is regarded as one of the most advanced political systems in the world concerning the promotion of gender equality. Its policies primarily aim to combat gender inequality and are often seen as exceptional political instruments compared to other European policies involving social regulations. For nearly four decades, the EU has imposed a series of norms and values on member states that surpass those in practice at the national level, creating a conducive environment for the development and mobilization of feminist movements.

The European Union's Integrative Vision for Advancing and Implementing the International Gender Agenda

In 1957, the construction of a European initiative focused on gender equality was not directly emphasized, especially in the context of a community founded on the implementation of a Single Market. European policies on gender equality were initiated and developed through treaties based on the gradual expansion of community competencies, in line with the enlargement of the European space, the political balance within the Council and the European Commission, and the increased emphasis on the role of women through key figures.

The Gender Equality Index is a tool used by the EU to measure the level of gender equality within the Union and its member states across various fields of activity. According to trends recorded in 2019, half of the member states failed to reach the European average on gender equality, prompting the European Parliament and the Commission, in the exercise of their functional responsibilities, to renew and rethink the vision for gender equality in the European context. Consequently, to give new momentum to gender equality and establish new political objectives in this area, the Commission developed a new EU Gender Equality Strategy valid for the period 2020-2025.

The Gender Equality Strategy outlines key actions for the next five years and commits to ensuring that the Commission will include a gender perspective in all policy areas of EU concern, at all levels and stages of the policymaking process. It will also address the phenomenon of intersectionality from a discrimination perspective, ensuring specific funding for this area through an increased number of programmes within the EU budget for the period 2021-2027 (Towards a Union of Equality – Gender Equality Strategy 2020-2025, 2020, p. 3).

This strategy for all of Europe, for all its member states, and for all its citizens embodies the vision of a space where women and men, girls and boys, in all their diversity, are treated equally and are free to pursue their chosen paths in life,

with equal opportunities to thrive, participate and lead in European society. However, it is important to note that this space is not geographically confined to the borders of the European continent. Through its development cooperation programmes and its foreign and trade policies, the EU positions itself as a crucial player in the international arena regarding gender equality.

The priorities within the strategy refer to the importance of establishing a Union of Equality, which promotes and supports equality for all and equality in all its senses (Questions and Answers: Gender Equality Strategy 2020-2025, 2020). These priorities are addressed in a dual manner, combining key actions to achieve gender equality with measures to streamline the integration of gender into all major EU political initiatives. The key actions essentially involve ending violence against women, combating gender stereotypes, eliminating gender disparities in the labour market, ensuring equal participation of women and men in various sectors of the economy, eliminating the gender pay gap and pension disparities, addressing gender discrepancies in family responsibilities, and achieving gender balance in decision-making processes and politics (Gender Equality Strategy, Achievements and Areas of Action, 2020).

On the other hand, it is necessary to include gender perspectives in all EU policies and processes, ensuring an adequate response to the needs of each gender while maximizing the multidisciplinary potential of EU citizens. To support the operational and technical integration of gender, the Commission has established a Gender Equality Working Group composed of representatives from all Commission services and the European External Action Service.

The establishment of a Union of Equality must serve as a common plea from all stakeholders, particularly focusing on eliminating gender-based violence and gender discrimination, fostering prosperity within an inclusive economic system, and ensuring equal meritocratic participation in decision-making and leadership roles across all sectors.

Implementing the key actions represents a shared responsibility, tailored to the specifics of each action, among EU institutions, the European Parliament, the Council and the European Commission, member states, representatives of civil society, social partners, and the private sector. In this regard, the Commission undertakes necessary actions to achieve the objectives of the current strategy and to ensure that gender equality is treated as a priority. The key actions outlined in this strategy are regularly updated and supplemented, with their implementation continuously monitored, and progress – including examples of best practices from member states – reported annually.

The annual reports are designed to include data from Eurostat and Eurofound, as well as indicators for measuring progress based on the EU's annual Gender Equality Index. The European Institute for Gender Equality (EIGE) will also provide detailed data and research to contribute to evidence-based policy-making and the updated information from EU institutions and member states.

In the sphere of external activities mentioned above, relevant to the research undertaken in this study, in addition to reaffirming the strategic commitment to gender through the adoption of the EU Gender Equality Strategy for the period 2020-2025, there was also the launch in 2020 of the third Gender Equality Plan (Gender Equality Plan III – GAP III) and the continued application of the EU's Comprehensive Approach to Implementing UNSCR 1325 and 1820 on Women, Peace, and Security. GAP III has been supported at the level of 24 member states, with the selected areas of action outlining the EU's clear vision regarding the essential elements that must be developed in the future for the organization's external action, including in situations of fragility, conflict and emergencies (A Union of Equality: Gender Equality Strategy 2020-2025, 2020, p. 20).

These elements include combating all forms of sexual and gender-based violence, integrating the Women, Peace, and Security agenda, strengthening the system of economic and social rights, empowering women and girls, advancing equal participation and leadership, addressing the gender dimension of the green economic transition and digital transformation, as well as health and reproductive rights (Presidency conclusions on the Gender Action Plan (GAP) III 2021-2025 – An ambitious agenda for gender equality and women's empowerment in EU external action, 2020, p. 6).

From the perspective of assimilating the provisions of UNSCR 1325 and its related resolutions, as well as from the perspective of gender integration, there are several documents at the EU level that regulate the essential aspects concerning the interplay between gender and security. Thus, to reinforce the EU's actions in this area, in December 2008, the Council of the European Union adopted the document titled *"The EU Comprehensive Approach to Implementing UNSCR 1325 and 1820 on Women, Peace, and Security"*, which covers the entire spectrum of the EU's external actions throughout a specific conflict cycle, from prevention to crisis management, peacebuilding, reconstruction, and development through cooperation.

As a parallel development of this key policy, it is noteworthy that the Council simultaneously adopted an additional operational document entitled *"Implementing UNSCR 1325 Enhanced by 1820 in the Context of the CFSP"* (December 2008). This document, based on previous operational documents related to this area, emphasizes new elements such as Resolution 1820 concerning sexual violence.

Essentially, we can consider that this document, combined with the Comprehensive Approach, forms the two pillars of the EU's policy on Women, Peace, and Security.

At the European level, EU institutions are responsible for implementing the integrative approach to gender equality, while at the national level, this task falls to the governments of member states. Therefore, although we acknowledge that gender inequalities still persist within the Union, significant progress has been made with the adoption of a proposal for a directive aimed at combating violence against women and domestic violence, as well as the launch in 2022 of the European Care Strategy, which addresses rights concerning the balance between private and professional life. Additionally, the EU Gender Equality Integration Strategy 2020–2025 has identified a series of additional advancements within the areas included in EU policies, among which we highlight climate change (The European Green Deal), artificial intelligence, health, energy, as well as the development of emerging technologies and digitalization.

The European Union is committed to promoting the long-term agenda of gender equality and women's empowerment in its external actions. In this regard, the EU has recently incorporated the principle of gender equality into its support for partner countries and adopted a measurable set of objectives regarding gender equality applicable to all European external initiatives, in line with GAP III.

As a novel element, the EU has implemented its own mechanisms, as well as through the EUMAM advisory mission in Ukraine, to support victims of gender-based violence and implement gender equality through three distinct projects (2024 Report on gender equality in the EU, 2024, p. 69).

The first project involves the establishment of a Ukrainian Women's Fund aimed at helping women's organizations strengthen their capacity to respond to crisis situations arising from acts of sexual violence. The second project provides support and expertise to the Prosecutor General of Ukraine through mobile justice teams to investigate cases of sexual violence occurring in armed conflicts. Finally, the third project, conducted in collaboration with the UN Secretary-General's Special Representative on sexual violence in conflict, primarily aims to support the Ukrainian Government with specialized advisors for women's protection, appointed at all ministry levels, in implementing national action plans regarding violence against women.

Current Challenges

Therefore, to ensure that the EU continues to be recognized as a global actor in paying particular attention to human rights, diversity, gender equality, and the widespread exercise of democratic principles, as well as to emphasize the importance

of its capacities regarding the allocation of its funds, several actions must be taken to maintain and surpass the recent positive dynamics and to provide responses that meet the demands of the ever-changing and evolving security environment.

Combining an enforceable system with coercive measures for member states, along with investing European funds in practices and projects that advance the integration of gender perspectives, leads, in our view, to a deeper and more prompt involvement of state actors in assuming and implementing gender considerations. This proactive attitude of states, in turn, contributes to achieving regional political and operational targets associated with gender, significantly aiding the generation of outcomes aligned with the legislative framework and the specialized human resources utilized to ensure long-term gender equality within the EU's sphere of influence.

CONCLUSIONS

According to the World Bank in 2024, men continue to enjoy more legal protection than women (Global Gender Gap, 2024, p. 36). For this reason, developments regarding the adoption of gender policies at the national level can no longer be minimized or dismissed, especially since gaps in implementation are widespread. Furthermore, out of the more than 100 countries recently analysed by the World Bank (Women, Business, and the Law dataset, 2024) and recognized as having national policies and programmes focused on addressing gender issues across multiple dimensions, only 53% report having sufficient resources allocated for their implementation (UN Women, 2023).

Thus, it is evident that both NATO and the EU must pay the price for peace, as more substantial financial investment ensures the durability of both organizations and their effectiveness in deterring foreign and hostile interventions. Budget allocation, even in the context of integrating gender perspectives across these innovative areas of action and interest for NATO and the EU, remains the *Achilles' heel*. It is because the true value and importance of the gender equality domain are reflected not only in its actual necessity for implementation but also in the concrete funding allocated to it.

The European Union is a unique and essential partner for NATO, as NATO Allies and EU members share the same values and have complementary and coherent roles that mutually reinforce each other in supporting international peace and security. Based on their long-standing cooperation, there is a desire to strengthen the NATO-EU strategic partnership, develop political consultations, and intensify cooperation on common interests such as military mobility, resilience, the impact

of climate change on security, emerging and disruptive technologies, human security, the Women, Peace, and Security agenda, as well as countering cyber and hybrid threats and addressing the systemic challenges posed by other states to Euro-Atlantic security.

For the development of the strategic partnership between NATO and the EU across multiple dimensions, including gender integration, the full involvement of Allies outside the EU in the EU's defence efforts is also essential. NATO recognizes the importance of leveraging diversity as a catalyst for a safer future, as well as the value of a stronger and more capable European defence that positively contributes to transatlantic and global security and is complementary and interoperable with NATO. Initiatives to increase defence spending and develop coherent capabilities that mutually reinforce each other, while avoiding unnecessary duplication, are essential for effectively and coherently leveraging joint efforts to make the Euro-Atlantic area safer in the context of comprehensive approaches to gender and all other emerging threats to international security.

In conclusion, we can assert that, from the perspective of the functioning mechanisms of the entities responsible for gender integration, both NATO and the EU stand out for their complexity and authenticity. However, although using different means and personnel with diverse qualifications and expertise, both organizations manage to fulfil their responsibilities regarding the promotion of the Women, Peace, and Security agenda based on common organizational values and international standards. This is eminently possible through the comprehensive approach to gender practiced at the level of security organizations, as well as through the constructive attitude that underpins the gender integration strategy, an attitude that facilitates the development of competence in the field and enhances this aspect as a necessary capability for completing the operational picture, as well as a key element in conflict prevention and, consequently, in ensuring international peace and security.

BIBLIOGRAPHY:

1. Bâtcă. M. (2023). *Raportul anual al secretarului general al NATO*, București. Agenția Media a Armatei, http://presamil.ro/raportul-anual-al-secretarului-general-al-nato/, retrieved on 12 September 2024.
2. Kjellström Elgin, K., Monaghan, S., Bjerg Moller, S. (2024). *Understanding NATO's Concept for Deterrence and Defense of the Euro-Atlantic Area.* Center for Strategic and Budgetary Assessments, Washington D.C., https://csbaonline.org/research/publications/understanding-natos-concept-for-deterrence-and-defense-of-the-euro-atlantic-area/publication/1, retrieved on 10 September 2024.

3. Loh, D. (2024). *China's rising foreign ministry: Practices and representations of assertive diplomacy*. California: Stanford University Press.
4. Ministry of Foreign Affairs, Permanent Delegation of Romania to NATO. (2024). *România în NATO,* https://nato.mae.ro/node/418, retrieved on 12 September 2024.
5. NATO (2021). *NATO Policy on Preventing and Responding to Conflict-Related Sexual Violence*. Brussels, https://www.nato.int/cps/en/natohq/official_texts_184570.htm, retrieved on 5 September 2024.
6. NATO (2022). *NATO 2022 Strategic Concept.* Madrid, https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf, retrieved on 3 September 2024.
7. NATO. (2024). *Military Voices on the Gender Perspective: A NATO Anthology*. Brussels, https://www.nato.int/nato_static_fl2014/assets/pdf/2024/6/pdf/20240614_NU_GENAD_Military-Voices-Anthol.pdf, pp. 4-18, retrieved on 8 September 2024.
8. NATO (2024). *NATO Policy on Women, Peace and Security (2024)*. Brussels, https://www.nato.int/cps/en/natohq/official_texts_227578.htm, retrieved on 3 September 2024.
9. NATO (2024). *Washington Summit Declaration*. Washington, https://www.nato.int/cps/en/natohq/official_texts_227678.htm, retrieved on 1 September 2024.
10. NATO. Allied Command Transformation. *NATO Warfighting Capstone Concept*. Norfolk. Virginia, https://www.act.nato.int/wp-content/uploads/2023/06/NWCC-Glossy-18-MAY.pdf, retrieved on 10 September 2024.
11. European Union, European Commission. (2020). *Towards a Union of Equality: Gender Equality Strategy 2020-2025.* Brussels, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0152, retrieved on 13 September 2024.
12. European Union, Council of the European Union. (2020). *EU Gender Action Plan (GAP) III – an ambitious agenda for gender equality and women's empowerment in EU external action*. Brussels, https://international-partnerships.ec.europa.eu/system/files/2021-01/join-2020-17-final_en.pdf, retrieved on 14 September 2024.
13. European Union, Council of the European Union. (2020). *Presidency conclusions on the Gender Action Plan (GAP) III 2021-2025 – An ambitious agenda for gender equality and women's empowerment in EU external action*. Brussels, https://data.consilium.europa.eu/doc/document/ST-13947-2020-INIT/en/pdf, retrieved on 16 September 2024.
14. European Union, Council of the European Union. (2024). 2024 *Report on Gender Equality in the EU*. Luxembourg, https://commission.europa.eu/document/download/965ed6c9-3983-4299-8581-046bf0735702_en?filename=2024%20Report%20on%20Gender%20Equality%20in%20the%20EU_coming%20soon.pdf, retrieved on 19 September 2024.
15. World Bank (2024). *Women, Business and the Law 2024*. Washington D.C. https://wbl.worldbank.org/en/wbl-data, retrieved on 21 September 2024.
16. World Economic Forum (2024). *Global Gender Gap 2024 Insight Report*. Geneva, https://www3.weforum.org/docs/WEF_GGGR_2024.pdf, retrieved on 20 September 2024.

ROMANIA AND THE USSR BETWEEN THE SPECTRE OF WAR AND DIPLOMACY IN THE EARLY 1930S

Museum Curator Valeria BĂLESCU, PhD
"King Ferdinand I" National Military Museum, Bucharest
DOI: 10.55535/RMT.2024.4.47

In the early 1930s, Romania received – through various diplomatic channels – numerous alarming news about the warlike tendency of the USSR. In parallel with this, diametrically opposite news also arrived in our country, which announced the intention of the Soviet government to negotiate with the Romanian state in order to conclude a non-aggression pact. The present article outlines some of the directions employed in the mentioned process.

Keywords: Romania; USSR; non-aggression pact; negotiation; Balkan Bloc;

SOVIET PROPOSALS FOR A REGIONAL PACT THROUGH TÜRKIYE

In the 1930s, it was known that both Ismet Pasha, the prime minister of Türkiye, as well as Tevfik Rüşdü Bey, the Turkish foreign minister, had a pro-Soviet orientation (Archives of the Ministry of Foreign Affairs/AMAE, file 80/1930, p. 189).

As far as Türkiye's position towards the Romanian-Soviet relationship was concerned, in the first part of 1930 (8 April) a news from Budapest informed that Rüşdü Bey[1] had knowledge of Soviet concentrations on Romania's eastern border and in the Black Sea basin, but he considered them to have only *"a demonstrative character"* (Ib., p. 192)[2]. Instead, he expressed his conviction that Soviet Russia would not give up *"reopening the Bessarabia question by any way and by any means, when the real situation would allow it to do so".*

More worthy of consideration for the subject that concerns us was the information that came directly from Türkiye, on 30 May 1930, from the Romanian envoy to Ankara, I. P. Carp (Ib., pp. 256-257). Following his audience with Rüşdü Bey, the Romanian diplomat concluded that in the view of the Turkish minister there were *"three dangerous areas"* in Europe, *"generating conflict"* and from which Romania was not excluded. Among those he listed: 1.) Danzig corridor area; 2.) The border area between Russia, Poland and Romania; 3.) The border area of the Kingdom of Serbs, Croats and Slovenes.

Rüşdü Bey was of the opinion that *"to eliminate the possibility of armed conflicts in these"* areas, it would have been necessary *"to conclude non-aggression pacts of the type called <Litvinov>"*, based on the principles of the *Geneva Protocol*. They could contain, in addition and as an essential condition, *"the obligation for the contracting parties to cooperate in collective sanctions, in case of aggression by one of the contracting parties against another signatory state of the regional pact".* Regarding the regional pact in the second zone, he added that it *"should be signed by the following states: Russia, Poland, Czechoslovakia, Romania and Türkiye".* The Turkish diplomat's belief was that the conclusion of such a document

[1] Tevfik Rüşdü Bey (1883-1972) was the foreign minister of Türkiye between 1925 and 1938.
[2] The news was transmitted by the Romanian minister from the Hungarian capital, Vasile Grigorcea, following discussions with his Hungarian counterpart from Angora, namely Minister Lajos Walko (1880-1954) – Hungarian politician and diplomat, Minister of Foreign Affairs of Hungary (during: 1925- 1930; 1931-1932), on the occasion of his return to his homeland (A.N.).

should be "*the first step in the work of pacification in this area"*, and, after that, it would be necessary to proceed to *"remove points of friction, especially the issue of Bessarabia"*. Rüşdü Bey thought that *"recognition of Russia of the incorporation of Bessarabia (to Romania) could be obtained through compensations"*. In this sense, he assumed the obligation for Türkiye to play the *"mediator role"* between Romania and the USSR, but not alone, and only alongside Czechoslovakia. The Turkish minister also promised to start such negotiations *"as soon as he finishes with Greece"* (Turkish-Greek negotiations were to follow), and that then he would *"concentrate all his efforts"* on the problem that he saw happening in three phases: 1.) the resumption of diplomatic relations between Czechoslovakia and Soviet Russia; 2.) the conclusion of the regional pact including the five signatory states; 3.) the Turkish-Czechoslovak action to eliminate the question of Bessarabia (Ib. , p. 257).

About this Turkish project, the French ambassador in Istanbul, Count Chambrun[3], expressed that it is not *"a too fertile imagination"*, but a *"chained ring of conventions"*, for Türkiye to consolidate its new national base. The idea of involving Czechoslovakia in the combination proposed by the Turks was not clear to Chambrun, because it was the country that did not have a common border with Russia. That is why he could not avoid the question: *"couldn't there be a desire to dislodge, to some extent, the Little Entente?",* a tendency behind which he suggested that Italy could have been (Ib., pp. 277-278)[4]. Mussolini's policy of isolating Yugoslavia at the time was obvious. Under his auspices, the Greek-Turkish convention was concluded. It was foreseen, also under the auspices of Italy, a *"Greek-Turkish pact of conciliation and arbitration, just like those concluded with Italy, Bulgaria and Hungary, then a naval arrangement and perhaps a Balkan pact, from which Yugoslavia would remain excluded"* (Ib., p. 279). Then, a regional pact would have followed on the Russian front, through the inclusion of Czechoslovakia and Romania, *"dislocating into several Little Entente"*. In fact, in connection with this, Count Chambrun had confessed to the Romanian envoy in Ankara that Tevfik had basically told him about six countries, he did not clearly remember one, but, apparently, he was thinking of Hungary. His opinion was supported by *"a symptomatic detail"*, observed at the banquet given by Türkiye at the Ankara Palace, following the Greek-Turkish convention, where they had been invited – apart from the Italian ambassador to Ankara – and the Russian ambassador, Souritz, as well as that of Hungary, Tahy.

[3] Count Louis Charles Pineton de Chambrun (1875-1952) was a French diplomat and writer. From 1928 to 1933, he represented France in Ankara and then became ambassador in Rome from 1933 to 1935.

[4] According to the telegram of the Minister of Affairs from Ankara, following no. 655/30 May 1930.

About Tevfik Rüşdü Bey and his claims as a skilled diplomat, Dimitrie I. Ghica[5], also informed, on 29 August 1930. He was talking about an interview given by Rüşdü Bey to the Soviet Agency *"TASS"* (taken over by the international press), which had produced *"something of a stir"*, because the Turkish diplomat had let it be understood that *"between Italy and Russia, Türkiye would be a co-signatory of a secret agreement of a political nature"* (Ib., p. 380). In fact, from the statement made, apart from the political interest that aroused him in a possible agreement, one could once again draw the conclusion that the Turkish foreign minister wanted to show the importance of Türkiye as a great power, on an equal footing with Russia and Italy, and, hence, his claim to influence in international politics.

And regarding the rumours of a Soviet attack on Romania, Ghica also conveyed the opinions of some secretaries of the Bolshevik embassy in Ankara, who accused *"in a fiery tone, through indignation and alcohol"* the nationalist circles in Germany for starting a *"campaign to propagate the aggression against Romania, in order to hamper the action of the Soviets to buy foreign currencies in order to implement the famous five-year industrial and agrarian plan"*. And following Rüşdü Bey's visit to the USSR, in October 1930, the same Romanian diplomat informed that, apart from the *"favourable"* (Ib., p. 346)[6] impression that the Turkish minister had made towards the country of the Soviets, as well as his delight in the *"intimacy"* of the Turkish-Soviet relations, with regard to Romania (Bessarabia), the head of Turkish diplomacy returned to the idea of a regional pact, which could have been concluded on the basis of the Litvinov Pact, but supplemented *"by applying the principles of the Geneva Protocol"* (Ib., pp. 445-446)[7]. Following that information, the impression of the Romanian diplomat was that Rüşdü Bey advocated *"regional pacts, conciliation, arbitration and neutrality treaties, to the detriment of alliances".* In this sense, he gave the example of the alliance between France and Yugoslavia, which led Italy to seek *"a counterbalance to this threatening force"*, thus grouping around it other states such as: Hungary, Bulgaria, Austria, whose Anschluss with Germany *"will admit if necessary"*, apart from any other solution.

[5] Dimitrie I. Ghica (1875-1967), during that period he was sent extraordinary and minister plenipotentiary to Rome (1928-1931), after which he was minister of foreign affairs between 27 August 1931-5 June 1932.

[6] Carp reported, on 10 October 1930, that industrialization was on the rise, that there were 400,000 workers in all branches, that the technical leaders were American and German, that they had travelled to the Black Sea on a new diesel engine ship built in the Leningrad shipyards; that the trains were running well and that, in general, the state's economy was progressing, although the standard of living was low.

[7] Communication by telegram no. 1552/17 October 1930, following telegram no. 1503 of 13 October 1930. After presenting the letters of accreditation to the President of the Republic, the Romanian Minister continued the conversation on the same topic with the Minister of Foreign Affairs from Türkiye.



Litvinov in Türkiye, October 1931, with Rüstü Aras
(https://commons.wikimedia.org/wiki/File:Litvinov...jpg)

On the other hand, during the meeting with I.P. Carp, Tevfik Rüşdü Bey emphasized the fact that Türkiye *"has a vital interest in ensuring peace between Russia and the neighbouring states, Poland and Romania"*. And because he was convinced that Czechoslovakia had the same interest, he insisted on the opinion that the two states *"could usefully play a conciliatory role"* between Romania and Russia. However, for it to materialize, according to the *"Rüşdü Bey"* scenario, it would be first necessary for Czechoslovakia to enter into normal diplomatic relations with the Soviet Union, and secondly, for Romania to show its willingness to *"offer Russia compensation for Bessarabia"*.

To the Romanian diplomat's question: *"What kind of compensations (?)"*, because he eliminated the territorial ones, considering that Bessarabia was *"a well-defined territory, of which no part can be ceded"*, and, also, *"giving up the treasury of the National Bank"* was out of the question, Tevfik replied *"that he has no idea either, but that the solution to the problem must be sought and found in this direction"*. Moreover, the Turkish diplomat had expressed his clear conviction that *"the Russian government cannot give up Bessarabia without compensation, because it would create a precedent, after which it would have to give up all its other territorial claims"*. He was referring to the Baltic States. To be even more convincing, the Turkish minister added: *"No one can deny that the Soviet Union*

is making amazing progress, especially as a military and industrial Power, and that the resumption of diplomatic relations with such a Power is becoming an imperative necessity for all states that have so far shown refractory".

Conciliating, Carp accredited the position adopted by the Turkish foreign minister, because he had just returned from the USSR and he was *"deeply convinced that the Soviet regime would not only endure"* but that it had overcome the greatest difficulties, now entering the *"phase of final consolidation"*, therefore his conclusion was that Türkiye's policy *"will therefore continue to be Russophile"*.

Rüşdü Bey seems to have taken seriously his role as a mediator between the USSR and the rest of the world, as Caius Brediceanu communicated from the Legation in Vienna, on 6 November 1930[8]. He reinforced his statement by a manifest gesture of Hamdi Bey, the Turkish envoy in the capital of Austria, on the occasion of the reception he had offered on the day of Türkiye. In that festive setting, the Turkish minister also introduced the Soviet ambassador Jurenew and his wife to the guests, which attracted the reaction of the other diplomats, who *"left the table and moved away (...), apart from the two high-ranking Austrian officials"*. The reaction of the diplomats – started at the initiative of the ambassadors from Switzerland and Hungary – was explained by the Romanian minister as follows: *"most of the foreign representatives here are indisposed to note that Hamdi Bey, the Turkish minister, is trying to patronize and introduce the Soviet representative into society, seeming to have instructions in this regard".* Apart from it, Brediceanu reported that all the members of the diplomatic corps to whom the Russian minister was introduced, *"shake hands with him on occasion or even talk to him, but avoiding closer relations"*; and even if the representatives of the Powers that had diplomatic relations with Russia invited Jurenew, *"his situation in society remains (...) precarious".*

In connection with *"an alleged mediation by Türkiye between Romania and the USSR"* also the envoy of Czechoslovakia to Ankara, Milos Kobr, asked minister Carp, on 12 November 1930 (Ib., pp. 475,477). The interrogation was related to the news that had reached him from Prague, following the discussions between his compatriot from Bucharest, Jizersky, with the Romanian diplomat Gheorghe Filality[9], *"that Türkiye had proposed to Romania its mediation in the Bessarabia issue"*. Carp denied the news and clarified his counterpart by telling him that Tevfik Rüşdü Bey had only presented him, on several occasions, *"his conceptions of a regional pact on the Russian front, but in a completely theoretical way, without any attempt of a concrete proposal"*, and that he transmitted all this in the country,

[8] Telegram no. 360.
[9] Gheorghe Filality (1864-1941), Romanian Minister at the Legation in Prague (Czechoslovakia).

avoiding, however, to express any personal opinion. Besides, Czechoslovak minister had revealed to him that he had also known about Rüşdü's plan, by virtue of which he had urged Beneş *"to start negotiations for the resumption of normal diplomatic relations with Soviet Russia"* (Ib., p. 476). Knowing all this, Kobr's conviction was that the attitude of the Turkish foreign minister only mattered to the extent that he wanted to appear *"as a personality who plays an important role in Europe"*. Without contradicting him directly, the Romanian minister did not agree with his point of view, but believed that it was a sincere desire of Rüşdü *"to see peace definitively ensured on the Russian front"*. What remained to be discussed, however, was whether his projects were the most effective.



15 October 1933, Ankara. Nicolae Titulescu, the Romanian Minister of Foreign Affairs, together with Tevfik Rüstü Aras, the Turkish Minister of Foreign Affairs. The visit to Türkiye resulted in the signing of the Treaty of Friendship, Non-aggression, Arbitration and Conciliation between Romania and Türkiye. In the picture, among others, are: Numan Menemencioglu, secretary general of the Ministry of Foreign Affairs of Türkiye, Ion Dragu, deputy director of the Romanian Press Directorate of the Ministry of Foreign Affairs, Nicolae Raicovicianu, Sergiu Nenişor and Dimitrie G. Buzdugan, personal secretaries of Nicolae Titulescu
(http://www.titulescu.eu /20/)

Trying to intuit the flow of information, Carp assumed that the news came from Rome, because Baron Aloisi (the Italian envoy to Ankara) had addressed him in the same sense. With an air of advice, he told him that *"Romania should resume normal relations with Russia, leaving the issue of Bessarabia to <sleep>"*. Carp replied: *"we don't wake it up, because for us it doesn't even exist, only the leaders of Soviet politics always stir it up. That is why we cannot resume normal relations with the Union of Soviet Republics without formal recognition on its part of the territorial status quo"*.

The Romanian Government also denied the news, on 7 November 1930, through Minister Mironescu[10], who declared the following to the press: *"It was published that the Turkish Republic would have proposed its good offices to the Romanian Government, in order to reach an agreement with a large neighbouring country. It is pure fantasy. We have the best relations with the Turkish Republic, but it was never about its friendly intervention between Romania and another country"* (Ib., p. 477).

However, Rüşdü Bey revealed the same ideas in Geneva, on 28 November 1930 (Ib., ff. 259v, 482, 483)[11], in front of Antoniade[12], the Romanian minister delegated to the League of Nations. Without detours, the Turkish diplomat had expressed his desire to reach the *"establishment of a Balkan block"*, which would include Türkiye, Greece, Yugoslavia, Romania and Bulgaria, but only under certain conditions. Among them he listed:

- the definitive rapprochement between Türkiye and Greece, which, according to his own expression, *"is as if accomplished following the conclusion of the last treaties between these two republics"*;

- the solidity of the Balkan block – for which it was necessary that *"each of the countries that will compose it erase any divergences not only between themselves, but also the other more serious ones with their other neighbours"*;

- regarding Romania, Rüşdü Bey believed that the agreement with Bulgaria was *"the easiest"; "harder"* but not impossible, was the one *"with Hungary and the Soviets"*. And if, according to his opinion, in Hungary *"the resistance can be cancelled with time, the question of the Soviets remained"*. Regarding their latter, Rüşdü Bey, through *"veiled words"*, as the Romanian minister further recorded, had let it be understood that during his last visit to Moscow he had made some suggestions about Poland and Romania, which the Soviets *"received favourably"*. And it would have been possible if it had been included in a wider agreement, which would even include mutual guarantees, in which *"Türkiye, the Soviets, Poland, Czechoslovakia and Romania would enter"*. Under those conditions, the Turkish minister insisted that the Soviets would have been willing to recognize the possession of Bessarabia, *"not a direct recognition of the treaty of 1920, he added, to which the Soviets could not be willing, they believe, without losing their prestige, but an implicit recognition, with the addition of a clause in the future treaty that the border issues between the two States will be regularized by good understanding, or something similar"*

[10] Gheorghe Mironescu (1874-1949) was president of the Council of Ministers of Romania in two stages: 7 June 1930 – 12 June 1930; 10 October 1930 – 17 April 1931.
[11] Telegram no. 74997/1930.
[12] Constantin Antoniade (1880–1954) was a Romanian jurist, writer, historian, philosopher and diplomat of Greek ethnic origin; he was Romania's representative at the League of Nations between 1928-1936.

(Ib., p. 483). The Turkish diplomat also explained that *"the Soviets would consent to the possession of all of Bessarabia (by Romania - A.N.) and that this clause would only be intended to protect them from the accusation that they simply received the fait accompli, imposed by the Great Powers"*. Instead, Rüşdü Bey believed that *"we should also give up our claims on the treasure stored in Moscow"*.

For the materialization of his proposals, Rüşdü Bey conveyed to Antoniade that he would come to Bucharest for diligence, but afterwards he declined his self-invitation (Ib., p. 260)[13].

Antoniade, in his report, did not forget to add that the news received from the Turkish minister had already been known to him from the Romanian minister in Ankara, but, nevertheless, he had listened with deference to the *"nebulous exposition"* of Rüşdü Bey, or *"wilfully nebulous in some parts",* without issuing any personal opinion. And he was, however, convinced that Rüşdü Bey wanted *"to offer his good offices as a mediator between Romania and the Soviets"* (Ib., p. 485).

Regarding the direct relations with the members of the Soviet delegation from the Preparatory Disarmament Commission, Antoniade specified, regarding the above, that *"no direct approach was made towards our delegation"*. And according to the instructions from home, he recorded that he was always *"reserved and had no relations with the members of that delegation other than strictly protocol and courtesy, and these were kept to a minimum"*. Instead, he reported a change in the general attitude of the members of the Soviet delegation. Unlike the other time, Antoniade remarked that they had shown themselves *"much more modest and conciliatory"*. They no longer came *"with extraordinary proposals, they no longer spoke, as they did at the previous sessions, for the audience and for propaganda, they no longer engaged in obstructionism and they no longer said impertinencies about the League of Nations or about the great <bourgeois> powers. They presented their points of view, but with enough modesty"*. The change of attitude of the Soviets had been noted *"by everyone"*, as had also been observed *"the growing concern of (their) leaders lately"*. It seems that the new change of attitude of the Soviets was due to the worsening of the internal situation in the Republic of Soviets, as some *"lesser"* Soviet delegates had confessed to their Genevan acquaintances. And at the moment when *"increasingly disturbing news began to trickle in from Soviet Russia (…), the first delegate, Litvinov, left Geneva".*

Even towards the end of the same year (28 December 1930), after Geneva and the Litvinov-Grandi meeting in Milan, Tevfik had kept his views vis-à-vis Romanian-Soviet relations. In this sense, he told Minister Carp: *"In Milan, Mr. Litvinov*

[13] Tevfik denies the news about a trip to Romania (telegram 1143/1931).

was reluctant", that is, he was not *"willing to negotiate on Bessarabia unless he saw a material or moral interest"*. As a result, Tevfik considered it necessary to consult with the Government in Moscow, but also with *"other governments"* (Ib., p. 260)[14] on this issue. On the other hand, Tevfik declared to Carp again, on 17 February 1931, that *"the issue of Bessarabia is for the Soviet Government exclusively a matter of prestige and that a formula could easily be found to manage these susceptibilities"* (Ib.)[15]. On the same occasion, the Turkish minister also expressed his concern about the rumour that Romania was strengthening its fleet, by buying warships from England, which would have caused *"the relocation of the Baltic (Soviet) fleet to Sevastopol"* and, thus, would have *"shaken the balance of forces"* not only in the Black Sea but also in the Mediterranean (Ib., file no 81/1931-1932, p. 34).

Tevfik's projects about the Balkan pact and the one on the Soviet front seemed to have been approved by France, as reported by the Romanian minister in Ankara, following the dialogue with his French counterpart, Count Chambrun. He opined that the French Government *"would not oppose"* any of the envisaged pacts, only on one condition, not to *"dislocate the Little Entente and, in general, the political system intended to maintain the territorial status established by the peace treaties".* Or, Rüşdü Bey wanted to replace the alliances with the system of regional pacts.

"These are, said Carp, two concepts diametrically opposed and difficult, but not impossible, to reconcile" (Ib., p. 511)[16]. However, his opinion was that, as conceived by Rüşdü Bey, the regional pact on the Russian front did not necessarily mean the *"dislocation"* of the Little Entente, the purpose of which was: the stability of the territorial status quo vis-à-vis Hungary; nor the weakening of the alliance between Romania and Poland, because it could be included in the new pact, just as the alliance between France and Belgium was included in the Locarno Mutual Guarantee Pact. But he believed that *"the reconciliation and framing of both systems requires a thorough preparation"* and, therefore, Rüşdü Bey needed it.

Later, however, Rüşdü Bey's conception would materialize, at least in part, through the expected Balkan Pact signed on 9 February 1934, in Athens, between: Türkiye, Greece, Romania and Yugoslavia.

[14] Carp thought it was about the Government in Rome, telegram no. 557/1931.
[15] See also telegram no. 13050/1931.
[16] Carp's telegram on 3 January 1931.



Photograph from the signing of some Military Protocols included in the Balkan Pact
(NMM Heritage, "Albums" Collection, inventory no. A. 1641, p. 41).

SOVIET PROPOSALS FOR A NON-AGGRESSION PACT THROUGH POLAND

Polish-Soviet relations had entered an *"acute phase"* since 26 April 1930, when a bomb dropped on the Soviet Legation in Warsaw, and the USSR accused the Polish Government of not having taken measures against *"known terrorist organizations (...), these being made up of White Russians and other foreign elements, who had enjoyed exceptional protection in Poland"* (Ib., p. 283)[17]. To them, were added the unfavourable comments from Moscow, about a *"future collaboration"* of a group of states against Russia, the interpretation that was given to the visits to Finland of the Polish Chief of Staff, of the Head of the Romanian Great General Staff, General Samsonovici, as well as of a French general.

However, in the last part of the year (2 October 1930), the special envoy of Romania in Warsaw, Alexandru Cretzianu[18], also informed about some rumours related to possible Soviet-Romanian negotiations for the normalization of relations, through Czechoslovakia, which would displease Poland (Ib., file 80/1930, p. 431). And, surveying the terrain in the Polish capital (a discussion with a high-ranking Polish official from Foreign Affairs), he had found that *"such an approach would seriously displease our Polish allies"*, because *"this case would be foreseen*

[17] News from Athens, 1 July 1930, from Langa-Răşcanu.

[18] Alexandru Cretzianu (1895–1979), during the period we are referring to, was the country's representative at the Romanian Legation in Poland; after that he was appointed a member of the permanent delegation of Romania to the League of Nations (1930-1932).

by the articles of the Treaty of Alliance". Through the resolution of 10 October 1930, the Romanian foreign minister gave clarifications to Warsaw, namely that there had been no negotiation, but only an understanding two years before, in the framework of a Conference of the Little Entente, where *"it was agreed that through that country to make a joint action"*, and since then nothing had been undertaken.

We find from the previously presented aspects that, in general, the representatives of Romania in the European capitals were equidistant in dealing with the sensitive issue we are presenting, thus bringing real services for their country, which was not exactly the case of the Romanian in charge of Affairs in Prague (appointed in 1928), Th. Emandi19.Over time, it seems that he had developed a real passion for Benes's political conceptions, regarding the resumption of diplomatic relations with the Soviets. He reflected this fact in the multitude and vastness of his reports (Ib., p. 431)[20] which, although important, were biased regarding Benes. Moreover, Emandi characterizes him as *"the only European personality who has real authority over the Soviets"* (AMAE, file 80/1930, p. 330).

The same happened through the report from the beginning of June 1930, when the Romanian foreign minister was warned not to be surprised *"by the future attitude of Benes"*, because he was *"badly impressed"* by the fact that the Romanian Government did not comply with the negotiations of 1928, the serious basis of which he had tried to arrange and from which the recognition of Bessarabia would have been *"undoubtedly resulted"* (Ib., f. 266). That is why Benes considered that *"he no longer has any commitment to us, being free to work on his own"* (Ib., p. 267). Insisting, Emandi added: *"There is no longer any doubt that the issue will be negotiated by Czechoslovakia, I had the honour to show you through my political reports that the current government combination (Romanian, A.N.) has two big problems to solve, namely: the economic issue and the relations with the Soviets".* And, thinking that it was *"of the greatest interest for the country not to remain isolated"*, he recommended that, in the matter of negotiations with the USSR, should be *"closely bound to our two allies"*, because both being Slavs, like Russia, *"an elementary precaution (was) absolutely indispensable".* Then, at another time, he stressed: *"It is no secret to anyone that there are insistences for Czechoslovakia to resume relations with Moscow. The foreign policy of the grouping of States*

[19] Theodor Emandi (1868-1942) was a Romanian diplomat and politician, of Greek origin. During the period we are talking about, he was Minister Plenipotentiary of Romania in Czechoslovakia (14 March 1928 – 15 December 1936). He remained in that post for more than four years, because N. Titulescu extended his appointment in Prague.

[20] See also reports from: 26 August 1930, pp. 308-336; 2 September 1930 (pp. 338-374); 2 September 1930 (p. 402); 13 September 1930 (p. 403); 5 September 1930 (p. 410); 2 December 1930 (p. 495) etc.

(Germany-Italy-Hungary) would of course profit if the states of the Little Entente, at odds over the Russian issue, would differentiate their points of view even more. The intermediary would be, who would think (?), Türkiye, which seeks to find the right moment, as the Turkish foreign minister has confessed. It is unnecessary to show how much goodwill Germany will show to these insistences" (Ib., p. 312).

With the obvious influence of the political environment in which he had been lived and less attentive to the real national interest, Th. Emandi, with regard to a protocol for the normalization of Romanian-Soviet relations, pointed: *"the basis of negotiations would have been the agreement between the two, from which it would appear that Russia recognizes (the union of) Bessarabia (with) Romania, renounces the treasury and any other claims. After this, it would have gathered the conference of four, which would have proceeded to organize the relations between the countries of the Little Entente and Russia"* (Ib., p. 316). It was, therefore, for the abandonment of the *"reprehensible passivity"* towards the Soviets and the change of tactics, in the sense of *"no longer being satisfied with the freedom we imposed on ourselves in the Russian matter, because, wherever, isolation and loneliness are powerless"* (Ib., p. 318). In such an idea, the Romanian minister in Prague thought that 1930 should be a positive year for Bessarabia, considering that, at the time, the Little Entente had consolidated and demonstrated its strength internationally (Ib., pp. 320-321). Admittedly, some of his opinions were indeed valid, but Benes was not as faithful to him as Emandi thought. He realized that fact by himself following an event that happened in August of the same year, which surprised and outraged the Romanian minister himself in equal measure. It was about Benes's meeting with the Romanian lawyer J. Th. Florescu, whom he knew during the exile in the First World War. The latter had come to Prague to participate in the International Congress of Criminal Law, on 25 August 1930. Then, following the meeting with Benes, he summarized the following conclusions to Emandi, regarding the involvement of the Czechoslovak foreign minister in the normalization of the relations of the Little Entante with the Soviets (and, obviously, as an intermediary between Romania and the USSR):

"1) That (Benes) is forced by the internal political situation to resume political relations with the Soviets by himself, he is free to do so, because he has reserved this freedom;

2) That currently he does not take them together with Romania, because it is more difficult than in 1928, when the Soviets demanded a plebiscite;

3) That for the time being he will only sign a Trade Convention with the Soviets;

4) That it is necessary to prepare the public opinion in the two states because, in any case, Czechoslovakia will remain a good friend of Romania from now on" (Ib., p. 374).

Upon learning it, Emandi was amazed that Benes had discussed *"categorical facts"* with Florescu, *"which, he says, during the morning he avoided".*

Leaving aside the particularities of the character of the Romanian minister from Prague, through those presented we tried to illustrate the fact that, indirectly, through various diplomatic ways, Romania was pressured by the USSR for the resumption of diplomatic relations in the terms imposed by it. On the other hand, it did not deny its status as a state promoter of the world revolution, for the purpose of which it was not afraid to attack the national security of the targeted state, in this case of the Romanian one. At the time, that fact was also highlighted by the Polish press, more precisely by the Krakow newspaper *"Czas"* (no. 249/29 October 1930), through the article *Attack against Romania* (Ib., p. 466)[21].

The publication revealed that Poland and Romania were considered by the Soviets to be key points in the realization of their plans to penetrate the western border for the spread of communism to the West, with the mention that Romania was the preferred target for a *"flank"* offensive. The motivation for such a hypothesis was related to a case of espionage discovered in Romania in 1930, which was considered *"one of the biggest ... since the war"*. *"Good specialists"* had thus been recruited, through which they had managed to *"penetrate even the high spheres of the Romanian security service"*, in order to learn important military secrets. Those aimed particularly the Polish-Romanian military convention and the exchange of views between Marshal Pilsudski and the Romanian Government (Ib., pp. 467-469). However, the plot being discovered in time, Romanian-Polish military relations could not be compromised, remaining even further to defend their important interest of *"maintaining common security vis-à-vis the neighbour"* in the east.

From the mentioned article, of interest for Romania were those aspects highlighted in the official sources and which referred to a war against Europe, especially through the neutralization of the Polish-Romanian alliance. The Polish official explained that the expected Soviet attack *"would not be done to rob Poland of a piece of land or (not only) to install a Soviet government in one of the neighbouring countries"*, but also to create *"over the neighbouring territories a way into the centre of Europe, into Germany and the Danubian countries, exploiting the political and economic ferments that exist there, and to bring about, with the help of the local Communists and perhaps even Hitler's partisans, a great social and economic revolution, with a word, to set Europe on fire".* But, because the experience of 1920 had shattered the Soviet hopes of a *"lightning"* passage through Poland, the USSR became more circumspect. And because the Soviets realized that the fight

[21] Article sent to Mironescu, on 1 November 1930, by the Romanian consul from Lwow (George Gallin).

with Poland could take a long time, they reoriented their strategic plan to conquer the west. Through the new vision, they had two possibilities: either to bypass Poland to the north, or to the south. And because the road through the Baltic States was considered, from a military point of view, *"quite risky and not very promising"*, then the southern route was more attractive, i.e. passing through Romania, more precisely through the area between Romania and Poland. The Soviets considered that the weakest point of the front from the Baltic Sea to the Black Sea was the sector between the Prut and Dniester, located on the line Kamenets-Podolsky-Cernauti-Kuty, where the Polish-Romanian territory comprised a narrow area of 150 km, with a single railway line between Poland and Romania. Their plan was to *"invade this area with strong forces"*, to separate Poland from Romania and penetrate into Subcarpathian Russia, *"undermined by the Bolsheviks and Russian agitations"*. From there they could then easily follow their path to Czechoslovakia and Hungary, making their way to Vienna. It was defined as a plan *"worthy of today's Napoleons of the Soviet army, who dream of a march to the Danube and to the Rhine"*. And in accordance with the geography of the place, it was considered *"that such a strike will have to take place especially on the Romanian territory, and not on the Polish one, which presents more difficulties in Eastern Galicia, thus exposing the Soviets to greater risks".* Through such an intervention, it was sought to separate the Romanian army from the Polish one and, further, destroy the Romanian one or throw it to the south. In establishing such a plan, the Soviets had considered that Romania was *"a weaker enemy"* than Poland. The idea was that, once a weak enemy was out of the game, they could then more easily defeat the stronger, but isolated enemy. And the case of espionage caught on Romanian territory revealed precisely that *"offensive of Soviet espionage in Romania".* That is why Romania was warned to prepare, to eradicate cases of espionage and to achieve *"a strong and careful control not only on the professional value of the people who deal with responsible activities, but also on their moral value"*, indispensable for *"maintaining an atmosphere of safety and trust not only in the country but also in the allied states".* The last point was emphasized knowing that *"for several years"*, Romania was going *"through a heavy internal political crisis"*, which was hoped to end along with the return of Carol II. Added to it was the extremely precarious economic situation, being the period of the world economic crisis, which caused the *"murmurs of the exhausted and indebted rural population"*, a situation precisely on which the *"hopes of the communist subversive elements"*, who sought the *"destruction of power"* and *"even of Romania's independence"*. Knowing all those things, through appropriate measures, it was hoped to thwart the Soviet plan to set Europe on fire, concluded the Polish publication.

If that was how things were in the subsidiary, officially, less than a month after the above news, the USSR made a proposal to Poland for the conclusion of a Pact of non-aggression and neutrality, as informed by the Romanian envoy from Warsaw, on 19 December 1930 (Ib., p. 260v)[22]. It was not a new approach, but a renewal of the one in 1928, by which the Soviet Power wanted to conclude a pact that *"stimulates the obligation for each of the contracting parties not to be part of any alliance directed against the other contracting party, in the event that one of the signatory powers would be attacked without provocation on its part".* Additionally, the USSR also wanted a commercial convention.

In order to accept the proposal, the Polish Government had set three conditions:

1. To be presented simultaneously to Romania and the Baltic States;

2. The provisions of the pact *"not to prejudice the obligations of the contracting states arising from the treaties and, in particular, towards the Covenant of the League of Nations"*;

3. At the same time, a *"conciliation and arbitration"* commission should be created. As far as the commercial convention was concerned, the Polish Government considered that it might be necessary to provide for the most-favoured-nation clause, which might be harmful, but its consideration should not, however, form an insurmountable obstacle to political negotiations.

Poland brought the Soviet proposal to the attention of the Romanian Government and the Baltic States, recommending, at the same time, that the commercial negotiations should be *"skilfully procrastinated"* until a result was reached regarding the non-aggression pact (Ib., file no. 81/1931-1932, p. 25)[23].

Especially, as far as Romania was concerned, before giving the final answer to the Soviets, the Polish Government considered it *"absolutely necessary"* that the formalities for the extension of the Romanian-Polish alliance treaty, which expired on 26 March 1931 (Ib.)[24], should start up to 1 January, so that the ratification would take place no later than 20 January 1931. Poland wanted to that time *"to stipulate the extension by renewal"* (Ib., file no. 80/1930, p. 500).

The Romanian government showed its willingness to accept all the proposals and suggestions of the Polish ally, on 22 December 1930, with only one inconvenience, that of operativeness, because Minister Mironescu was out of the country for 15 days (Ib., p. 501). Then, the negotiations seemed to follow their normal course, but *"a regrettable press indiscretion occasioned a denial by the agency <TASS>,*

[22] See also telegram no. 78971/1930.

[23] Letonia, see the Riga report of the Romanian Legation, dated 2 January 1931.

[24] Memoir on the consequences of the indiscretion made by the *"Lupta"* newspaper, relative to the Polish-Soviet negotiations (pp. 24-28).

which denied the existence of the negotiations" (*Le Temps*, 7 January 1931). The *"indiscretion"* appeared under the signature L. Artemie (AMAE, file no. 81/1931-1932, p. 25), in the newspaper *"Lupta"*, on 4 January 1931, therefore, before the start of the negotiations for the extension of the Romanian-Polish guarantee treaty, and recorded both the propositions, the Soviet one, and Poland's response, with the mention that the news had been found out *"accidentally", "from a good diplomatic source from abroad".*



5 Ianuarie 1931

4 Lupta 4 ian.

Alianța româno-polonă

Rusia intervine cu o propunere foarte importantă

Intrevederea Mironescu-Zalewski

In cursul lunei Februarie expiră tratatul de alianță dintre Romănia și Polonia.

Tratativele în vederea reînnoirii acestui pact urmează de cătăva vreme pe cale diplomatică și este neîndoios că ele vor duce la un perfect acord.

In ultimul timp a intervenit însă, independent de aceste tratative un fapt nou menit să accelereze trativele pentru încheierea noului tratat de alianță.

Intr'adevăr, după cum arată informațiunile pe cari le deținem întâmplător dintr'o bună sursă diplomatică din străinătate, guvernul sovietic a făcut acum câteva săptămâni, guvernului polon o propunere pentru încheierea unui pact de neagresiune polono-sovietic, care ar asigura o neutralitate perpetuă între cele două state semnatare.

Deasemenea statele semnatare s'ar angaja să nu participe la nici o alianță îndreptată împotriva celeilalte puteri.

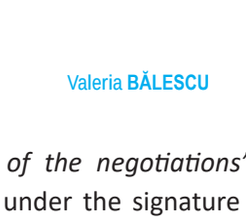
După cum se vede, e vorba de un pact a cărei importanță ar depăși-o chiar pe aceia a pactului Litvinoff, care ar asigura pacea între Polonia și Rusia.

ĂSPUNS POLONIA

a polonez luând cu- e această propunere

a guvernului sovietic, s'a declarat gata să trateze încheierea pactului, condiționând însă aceasta de introducerea unei clauze care să facă posibilă extinderea lui și asupra tuturor semnatarilor pactului Litwinoff.

Până în prezent, guvernul so-



D. ZALEWSKI

vietic nu a răspuns încă la această cerere a Poloniei. Se crede însă că Sovietele vor accepta sugestia Poloniei pentru a face posibilă încheierea unui pact, în genul celui semnat la Moscova, din inițiativa d-lui Litwinoff.

SOLIDARITATEA ROMÂNO-POLONĂ

După cum se vede, Polonia a avut și de astădată aceleași atitudine leală pe care a arătat-o față de Romănia și cu prilejul semnării pactului Litwinoff.

Este deci explicabil că, pentru a accentua aceasă solidaritate între cele două țări, tratatul de alianță polono-român să fie reînoit încă înainte de începerea eventualelor tratative polono-ruse.

Credem a ști că noul tratat româno-polon va fi încheiat până la finele lunei Ianuarie.

In acest scop ar avea loc în străinătate o întrevedere între d-nii Zaleski ministrul de externe al Poloniei și Mironescu, președintele consiliului și ministrul de externe al Romăniei.

Cu acest prilej se vor pune la punct toate chestiunile cari privesc cele două state.

IMPORTANȚA PACTULUI

După cum se știe pactul Litwinoff a fost încheiat între Rusia și statele limitrofe pentru a anticipa aplicarea pactului Kellogg, în această parte a Europei.

Noul pact, propus de guvernul sovietic ar avea pentru noi o importanță cu mult mai mare decât pactul Kellogg deoarece ar asigura în mod efectiv pacea în Estul Europei și-ar risipi odată pentru totdeauna impresia care dăinuește de atâta vreme în lumea politică internațională, că Rusia ar constitui o permanentă primejdie de războiu.

L. ARTEMIE

The "indiscretion" of the article in the Lupta newspaper, dated 4 January 1931
(AMAE, collection 71, 1920-1944, USSR, volume no. 81/1931-1932, p. 3.)

The indiscretion caused *"the most vivid and justified surprise"* in Warsaw, and the Polish foreign minister, Zaleski, declared that *"under such conditions it will be very difficult for him to make any more communication of the nature in question".* The consequences were that the Polish-Soviet negotiations were interrupted, and the Moscow Government provided a disclaimer, through the *"TASS"* agency,

which clearly meant that the Soviets intended to withdraw the proposal made. The incident was not insignificant, especially for the Government in Warsaw. It had been put in a rather delicate position vis-à-vis Moscow, because it demonstrated that it was keeping Bucharest informed of the confidential negotiations it was conducting with the USSR. Minister Mironescu also expressed his indignation at what happened, through the telegram of 8 January 1931, in which he expressed that *"the indiscretion (...) prevented for a time, which may be long, the relaxation that had been prepared to the East. All the diplomatic action that we started is now thwarted. Russia reacted and we can expect it to officially withdraw its proposal these days"* (Ib., p. 26).

For Romania, the incident was even more harmful, all the more so since, in Ankara, the USSR ambassador in Türkiye, Suritz, in the conversations he had with his Polish counterpart, had shown himself eager for a rapprochement of Soviet Russia with Romania and Poland, in order to *"conclude a pact by which, implicitly, the annexation of Bessarabia would be recognized"* (Ib., file no. 80/1939, p. 360)[25]. He said that the new pact would be a development of the *"Litvinov"* Pact, by adding some guarantees, which *"would not oblige the signatories to military cooperation with the attacked State against the aggressor State"*, but only to preserve neutrality: military cooperation would not be than optional.

But the above wording was not accepted by the Polish Government, in order to manage the susceptibility of the Soviets, who would be *sur le qui-vive* (on the alert) as a result of the *"indiscretion".* Nevertheless, Poland was still willing to continue the negotiations, for which the Polish minister from Moscow, Patek, arrived in Warsaw, on 17 February 1931, to establish a *"detailed program for conversations with the Soviet Government"*, following his proposal for conclusion of the Non-aggression Pact. It was estimated that in this way the Soviets wanted *to "create a new argument against the so-called Russian clause of art. 8 of the Covenant of the League of Nations, with a view to the Conference on Disarmament, an argument that could have a great propaganda value"* (Ib., file no. 80/1930, p. 261)[26].

[25] See also telegram no. 1143/1931.
[26] From the Warsaw Legation, telegram no. 9712/1931.



Warsaw, October 1933. On an official visit to Poland. Nicolae Titulescu, the Minister of Foreign Affairs of Romania, is received by the President of Poland, Ignacy Moscicki, and the Minister of Foreign Affairs, Josef Beck
(N. Titulescu, Politica externă a României/Romania's foreign policy (1937), George Potra, Constantin I. Turcu, Ion M. Oprea (eds.), Editura Enciclopedică, București, 1994).

As for the attitude of the Baltic States, although they were in principle *"favourable to an anti-Soviet bourgeois bloc"*, it was believed that, due to the state of economic crisis they were going through, they could be attracted to Russia, through economic proposals aimed at easing their economic situation[27]. The bilateral commitments of the Baltic States with the USSR had already caused Poland to declare that it would never accede to the Protocol of the new Pact, even though Poland had undertaken to submit it to the attention of the Foreign Ministers of Latvia and Estonia. In such a situation, *"one could no longer count with the same certainty on the continuation of the solidarity of the neighbouring countries with Russia"*, because only the Governments of Bucharest and Warsaw remained in discussion, to *"invoke the exception of the Soviet neighbourhood"* (AMAE, ib., file no. 80/1930, p. 261v)[28] at the Disarmament Conference. It was, thus, an obvious diplomatic victory for the Soviets, obtained following the economic pressure in the Baltic States, as a result of the dumping policy.

[27] The Romanian Legation in Riga, on 20 March 1931, reported that the Soviet proposal to Latvia and Estonia tended to lead to the conclusion of bilateral commitments, whereby each contracting party is obliged not to participate in any political or economic agreement directed against the other party. Considering the changes in the governments in Riga and Tallinn, it seemed that Poland no longer intended to insist that the negotiations with the USSR, for the signing of a non-aggression pact, should be carried out simultaneously with the other signatory states of the Litvinov Pact, but it was satisfied only to condition the entry into force of the accession agreement of the other governments (Riga Legation, telegram no. 13296/1931; Bulletins of the Eastern Political Directorate: no. 4, p. 45; no. 5, p. 39).

[28] See also the telegrams from Riga no. 17389 and 20175/1931.

Regarding the situation in Romania in the mentioned conjuncture, Patek, who had returned to the capital of his homeland and met his Romanian counterpart in Warsaw, had the opportunity to directly convey the message to Litvinov, with a view to the normalization of Romanian-Soviet relations. Patek had taken advantage of the Soviet dignitary's visit to the Polish Legation in Moscow, to remind him of a promise made two years before, in front of the Romanian minister Davila, to resume conversations on the aforementioned topic. Therefore, Patek pointed out to him that he had been waiting for the resumption of the conversation since then, but Litvinov, dryly, replied: *"We cannot restart any kind of negotiations with Romania, which owns a territory that belonged to us. If Romania wants, it will resume its initiative of negotiations. We do not want to reopen a negotiation in which we would have nothing but to lose"* (Ib., file no. 81/1931-1932, p. 39)[29].

SOVIET ATTEMPTS AT DIRECT NEGOTIATIONS WITH ROMANIA THROUGH THE LONDON DIPLOMATIC CHANNEL

Because the USSR had not obtained the expected results in the recorded diplomatic attempts, it initiated negotiations with Romania in the first part of 1931, on the London channel, through the Romanian diplomat D.N. Ciotori. He had been contacted by A. Lias, the foreign policy editor of the newspaper *"The Christian Science Monitor"* (London Branch), who, following a conversation with Bogomoloff, counsellor of the Soviet Embassy in London, conveyed the message to the Soviet dignitary for our country, namely that *"the Soviets would like to reach an agreement with Romania, if a formula could be found so that they could escape <with a clean face>"* (Ib., p. 102). Ciotori then tried to *"probe"* Soviet aspirations through F.E. Wise, the member of the House of Commons, but also through a friend, Wickham Steed. The conclusion was that, indeed, the Soviets wanted *"an agreement with Romania and that they would have preferred direct negotiations <to stop paying political commissions to intermediaries>"* (Ib., p. 103).

At that time, Ciotori had informed the country about the message, through N. Iorga (located in France, at Fontenay-aux-Roses), for which the historian informed him, on 6 March 1931, that the Romanian authorities had determined that he, Ciotori, went to Moscow with authority to discuss only *"the return by the Soviets of the archives and property of our museums"* (Ib.). Transmitting the information to the Soviet representative, through the same source in London, the answer

[29] See also the telegram from Warsaw no. 508/20 February 1931.

reached him only on 23 April 1931, through F.E. Wise, after which he directed him to Bucharest (via phone no. 24, 25/24 April). Following the approach, Ciotori was called to the country for instructions, *"as soon as the formalities are fulfilled"*, that is, obtaining the necessary documents and visas from the Soviet Embassy, in order to travel to Moscow. Then followed an exchange of telegrams between Ciotori and the country's officials, as a result of which the Romanian diplomat was in a bit of a mess, because not having received the power of attorney from the country, he could not obtain the *"formalities"*, a fact for which he sent new clarifications to the Foreign Affairs, which he formulated as follows:

1. the initiative of the discussions *"does not belong to us in any form"*;

2. *"absolutely nothing was discussed elsewhere, except whether the Soviets consent or not for us to have a secret discussion with them in order to seek the basis of an understanding which will, then, be completed in an official conference"*; and as a supplement, to avoid any doubt, he added: *"The Soviets do not agree to separately discuss the restitution of the archives and the assets of our museums, the authorization requested to discuss the restitution of the archives was – for the Soviets – only a pretext. The general authorization was essential and the Russians asked for it in order to discuss all the disputed issues (Bessarabia does not enter into the disputed issues)"* (Ib., pp. 105-106).

In the period that followed, no viable result being reached, communication with the London channel ceased.

FRANCO-SOVIET CONNECTIONS FOR THE CONCLUSION OF A NON-AGGRESSION PACT WITH THE REGULATION OF ROMANIAN-SOVIET RELATIONS

The interest in the normalization of Romanian-Soviet relations was increased on the part of the USSR, not for the sake of Romania, but because it was conditioned by the conclusion of other diplomatic relations. It was clear from Carp's report, sent from Türkiye, on 12 September 1931 (Ib., pp. 116-118)[30], following the discussions he had with Count Chambrun. The content of the document also makes us understand why, in the intermediate negotiations that were to come, for the normalization of Romanian-Soviet relations, Romania will be pressured by France and Poland.

In the Soviet political calculation, of guaranteeing security on the part of the West through non-aggression pacts, aiming at the successful conclusion of such

[30] Report no. 1441, extracted from: *Therapia*/6 September 1931, registered under no. 53149/12 September 1931.

a Franco-Soviet agreement, during that period the negotiations stagnated. And amid the deepening economic crisis, Count Chambrun testified that France had been forced to *"give up the defence policy against Russian dumping"* (Ib., p. 116), due to the progressive worsening of France's trade balance with the USSR (the difference against France was 100 million francs). Therefore, France had lifted all prohibitive measures to combat Soviet dumping and had considered it more appropriate to conclude a trade treaty. But, because the complexity of the economic problems had proven to be irreconcilable, both sides had felt the need to conclude a *"political agreement simpler and faster to achieve"* (Ib., p. 117). On this basis, secret negotiations were conducted between Barthou and the Soviet ambassador in Paris. A common point of view had been reached, but an *"indiscretion"* appeared in the American press *"suddenly raised the question of the connection"* of those negotiations with those followed between Warsaw and Moscow. About it, the same Chambrun reported: *"In the beginning, therefore, the connection does not seem to have existed, the starting points of both series of negotiations being completely different. At first, France aimed only at balancing the trade balance with the USSR, but the indiscretion committed, however, complicated the problem in such a way that, today, the conclusion of the Franco-Russian agreement depends on the Polish-Russian agreement, and the Polish-Russian agreement depends on solving of the relations between Romania and Russia".*

Under the given conditions, France had no other solution but to conclude a new *"Karahan Protocol"* (from 1929) for two years, and the French count said that he would ask for clarifications in Paris if, in relations with the Soviets, *"he has to touch upon the problem of resolving the relations between USSR and Romania"* (Ib., p. 118), without which there could be no Franco-Russian, Polish-Russian non-aggression pact, or multilateral pact of mutual guarantee, which Tevfik Rüşdü Bey must have to support.

On this topic, in the following year, the pressure would increase on Romania, for the *"smoothing"* of Romanian-Soviet relations, which seemed quite difficult, given that the parties remained irreconcilable in supporting their points of view. And, to stay in the same register, the situation was thus expressed in Ankara, by Husein Raghib Bey, former ambassador to Romania. On the date we are talking about (30 October 1931) he was Türkiye's envoy to Moscow. In a meeting with the Romanian minister, Carp, on the occasion of the National Holiday of Türkiye, Raghib Bey clearly conveyed to him that *"there is no possibility of rapprochement"* between Romania and the USSR as long as *"there is no change in the position taken by each"*

between the two neighbouring states. And, more explicitly, he formulated: if the Soviet state *"fully maintains its point of view and neither Romania wants nor can make any concession on the issue of Bessarabia"*, in the given situation, it is no possibility of contact.



Bucharest, June 1934. Nicolae Titulescu, Romanian Minister of Foreign Affairs, together with Jean Louis Barthou, French Foreign Minister, accompanied by other Romanian and foreign officials, at the Tomb of the Unknown Hero in Romanian Capital (Titulescu, ib.).

During the same celebration, Rüşdü Bey wanted to present Litvinov to Carp, but the Romanian minister declined his offer, not being authorized to do so. Thus, the official Romanian-Soviet contacts will be postponed, until, over pressure and sterile negotiations, under the conditions of the debates in the *Disarmament Conference,* within the League of Nations, the harmonization of relations between the two states will be reached by signing the *Conventions defining aggression from London*, on 3-4 June 1933. It was an important step that, a year later, also led to the normalization of Romanian-Soviet diplomatic relations, on 9 June 1934.

BIBLIOGRAPHY:

1. Arhivele Ministerului Afacerilor Externe/Archives of the Ministry of Foreign Affairs/ AMAE (1930). Collection 71/URSS, Relations with Romania, file no. 80, p.189, 192, 256-257, 259, 266, 267, 277, 278, 279, 312, 316, 318, 320, 321, 330, 374, 380, 431, 436, 445, 456, 466, 469, 471, 476, 477, 482, 483; file no. 81/1931-1932, pp. 24-28;

(1931). Collection 71/URSS, Relations with Romania, file no. 80, pp. 260v, 261, 283v, 485, 500, 511; file no. 81/1931-1932, p. 28.
2. Eastern Policy Bulletins no. 4, p. 45; no. 5, p. 39.
3. *Le Temps*, 7 January 1931.
4. Romanian Legation in Riga (1931). Telegram no. 13296/1931.
5. National Military Museum Heritage, "Albums" Collection, Inv. A. 1641, p. 41.
6. Titulescu, N., *Politica externă a României (1937)* (1994). Ediție îngrijită de: George Potra, Constantin I. Turcu, Ion M. Oprea. Bucureşti: Editura Enciclopedică.
7. https://commons. wikimedia.org/wiki/File:Litvinov...jpg, retrieved on 22 July 2024.
8. http://www.titulescu.eu /20/, retrieved on 11 August 2024.

POLITICAL, ECONOMIC, AND MILITARY COOPERATION BETWEEN ROMANIA AND THE SUCCESSOR STATES OF FORMER BRITISH RHODESIA (ZAMBIA AND ZIMBABWE) BETWEEN 1970 AND 1989

Colonel Associate Professor Andi Mihail BĂNCILĂ, PhD
"Ferdinand I" Military Technical Academy, Bucharest
DOI: 10.55535/RMT.2024.4.48

Despite a rich international bibliography dedicated to the fight for national independence of African states and their evolution in the postcolonial period, the contribution of the Romanian state to the achievement of this important objective is completely neglected. An interesting chapter for our national history, little known to the public, is the military and economic collaboration of Romania with the successor states of the former British provinces of North and South Rhodesia, the current states of Zambia and Zimbabwe. That financially risky approach had all the chances to become a viable project to position Romania among the states with influence on the African continent.

Keywords: Rhodesia; defence industry; military collaboration; national liberation; anticolonial struggle;

INTRODUCTION

One of the most important points on the foreign policy agenda of the two superpowers, the United States of America (USA) and the Union of Soviet Socialist Republics (USSR), in the second phase the Cold War was to identify the means by which they could extend their influence on the *"third world"* (Tomlinson, 2003, p. 207)[1] of which the states on the African continent were also part. Their entry into this space was to come at the expense of the former colonial powers, Great Britain and France, which immediately after the Second World War hoped to support the reconstruction of their own economies devastated by conflict through raw materials and labour available in the territories that legally belonged to them. Even though in the first phase of the Cold War the USA seemed to support, financially and militarily, the maintenance of the two European empires (Darwin, 2021, p. 504)[2], subsequently, despite declared intentions to support Great Britain and France, the Americans invested enormously in supporting the national liberation movements. It was most likely intended to break the economic monopolies that France and Great Britain had in the colonies and to open the markets of those new states to the free economy in which the USA dictated the rules of operation. The weakness manifested by the European metropolises created the necessary conditions for other states with different levels of economic development to try to develop political, military and especially economic relations with the new states on the African continent. One of the states that risked investing in supporting those movements was Romania, which most likely wanted to create an outlet for many of its products lacking competitiveness in the international market.

THE INTERNATIONAL CONTEXT THAT ALLOWED THE ANTICOLONIAL STRUGGLE TO START

Despite a moment of hesitation immediately after the end of the Second World War for the political leadership of the United States of America, it had already become clear that the British Empire would no longer be able to afford to financially

[1] The term *third world* described the community of states that at that time were not ideologically aligned to one of the two political-military blocs: the communist world ruled by the USSR and the *"free"* world led by the USA. In the first phase of the Cold War the interest of the two superpowers was centred on strengthening their power in the European territories where they deployed their armed forces. (A.N.).

[2] The funds made available to the two colonial powers were considerable for that period. Fearful of a possible expansion of the influence of the USSR in Iran and the Persian Gulf states, the USA had allocated, following the end of the war, about 1 billion dollars annually to defend the British Empire's interests in the Middle East. (A.N.).

and materially support the installed political leadership in the various provinces of the empire. This fact was recognized even by the British who claimed that in many situations the expenses already exceeded the possible profits that could be obtained there. Lord Curzon, a former foreign minister of the British Empire, had declared since the end of the First World War that Britain's military presence in the Middle East, regardless of future earnings from oil exploitation, was too expensive: *"expenses can no longer be sustained"* (Frankopan, 2019, p. 378). Considering the potential for economic growth in the Middle East, which could be sustained through the exploitation of oil, and comparing it with low expectations for future exploitations in various African colonies, we can conclude that the Great Britain was already planning to cut its spending by abandoning some of these colonies. The thus created opportunity was grasped by both rival powers and Western-schooled leaders of the indigenous population who were willing to engage in military conflicts to take political power from the hands of the British.

As regards the support of the national liberation movements, the position of the political leadership in the USA coincided with that of the USSR, both of which were ready, regardless of the costs, to provide material and financial aid to these local leaders in the hope that they will succeed in expanding their ideology and model of economic development in this space. This seemingly disinterested aid was the perfect opportunity the two superpowers used to develop their trade with the arms produced by their defence industry. The best example is that, between 1967-1978, the Soviets and the Americans delivered more than 4 billion dollars' worth of weapons to African states (2.7 billion USSR and about 1.6 billion USA) (Zaayman, 2010, p. 140). The US military presence in Africa was recorded as early as the Second World War, when the American armed forces decisively contributed to the evacuation of the Nazi armed forces from the northern part of the continent. That moment was speculated by the Americans to strengthen their relations with some of the North African leaders to whom some of the weaponry used during the conflict was distributed. For the USSR this step was an element of novelty, the political leadership of this state being willing to unconditionally deliver several types of weapons at sometimes lower prices than the price of production. Figures indicate that between 1960-1970 the value of Soviet arms deliveries increased from just 150 million dollars to more than 2.5 billion (Ib., p. 141).

Under the pressure of new ideas and with the military support of the USSR and the USA in many of the territories of former colonial empires, paramilitary groups were formed that triggered an unbroken string of conflicts. Very few specialists supported the idea of forming national states built around the European idea

of nation. The states established on the territory of former empires had borders that were inconsistent with their ethnic structure and, not infrequently, tribal peoples or communities were divided by arbitrary borders drawn on the ruins of former provinces in the colonial era (Stockwell, 2007, p. 243). This aspect, combined with the very low level of education and civic awareness, produced a real tragedy, with most of the new states being thrown into bloody civil wars. Many of the African leaders were willing to work together to achieve this goal, and would later militarily settle their existing divergences. It generated a rapid increase in military needs, with arming becoming one of the major objectives of the new leaders.

Those were the new circumstances in which political leaders of developing countries, such as the central and eastern European states in the area of influence of the USSR, which shyly started to develop their military sectors began working with various African leaders to whom they offered military support. Armed with weapons procured from around the world, these paramilitary groups, still led by tribal leaders, starting in the 50s of the past century, became very active and managed to cause considerable losses to armed groups led by military leaders of European origin (Darwin, p. 535) and subsequently to gain not only national independence but even a privileged position, compared to the neighbours. The richness of the soil and subsoil of African states very quickly became their main drawback. Both the former colonial powers and the two superpowers chose to support the bloody dictators they armed to be able to impose themselves in front of the contenders supported by rival powers. The very large number of conflicts that erupted created the necessary conditions for states that previously lacked the means to promote their interests in this area to enter the African market for arms and resource exploitation. Alongside PR China that, despite its economic and military underdevelopment at that time, harboured great ambitions, on the African market entered with their products the Soviet satellites from Central Europe, among which was Romania.

The Romanian state took full advantage of the opening of those colonial monopolies and tried to establish economic relations with a part of those states. Following a model of co-operation already established by the two superpowers and the two former colonial powers, Romania chose to support some of the African political leaders with the necessary elements to strengthen their power. The first visit by a high-ranking Romanian official to Africa took place in May 1970. Corneliu Mănescu, the Romanian Minister of Foreign Affairs, conducted a tour of Central and East African states with the declared goal of developing lasting economic and political relations. Between 3 and 26 May, he succeeded in establishing initial contacts with officials from the new states that had emerged on the African

continent: Gabon, Congo, Cameroon, Nigeria, Burundi, Tanzania, and the Malagasy Republic (Madagascar) (Melinescu, apud Hlihor, 2024, p. 60). Mănescu's visit was merely a preview to the future relations between the Romanian state and many African countries that had either gained independence or were in the process of proclaiming it. The first African leader to recognize the emerging opportunity was Robert Mugabe, head of the paramilitary organization ZANU (Zimbabwe African National Union). He sought to strengthen his position against Joshua Nkomo, leader of ZAPU (Zimbabwe African Peoples Union), who was also fighting for independence from Britain in the province of Southern Rhodesia. Mugabe's quick response to the Romanian leader's invitation stemmed from his concern over his internal rival, Nkomo, who had already secured external support from Ethiopia.

ROMANIA'S CONTRIBUTION TO STRENGTHENING THE NATIONAL INDEPENDENCE OF THE STATE OF ZAMBIA

On 24 October 1964, when Northern Rhodesia became Zambia, it declared its independence from the British Empire, having a population of about 2,400,000 people on its territory, of which 74,640 were settlers of European origin (Shurmer-Smith, 2011, p. 83). That minority, which had received direct support from the British government, owned the vast majority of the agricultural land and mineral resources of the young state. That situation generated considerable dissatisfaction among the native population, which exerted pressure to achieve the nationalization of the lands owned by them (Brown, in Evers, Spierenburg, Wels, 2005, p. 82)[3]. As a result of those reforms, the new president of Zambia lost the support of the Western states, which, like other leaders of the new African states, he accused of destroying the African ethnic space and implicitly their way of life. According to his point of view, it generated material deprivation and economic backwardness. Within the new political context that was formed and the interest that the socialist states manifested for the development of political-economic relations with the African states, he addressed the president of the Romania, Nicolae Ceaușescu to get the economic support he needed. According to documents preserved in the archives of the Central Committee of the Romanian Communist Party (RCP), Romania had become a state capable of providing not only the necessary materials for the struggle against colonialism but also the political and ideological support needed

[3] During the colonial period, a large portion of the native population in Zambia was relocated to the outskirts of farms owned by white settlers, being allocated small plots of land insufficient for producing the food necessary for the growing population. In that way, the British managed to achieve a second economic objective, namely to ensure the labour force required for large agricultural operations. (A.N.).

for the reform of the Zambian state in accordance with socialist principles.

In a letter addressed to the Romanian president by his Zambian counterpart, Kenneth Kaunda, sent on 10 November 1970 (ANIC, p. 14), it was noted that the relations between the two states had already laid the foundations for the development of solid technical and economic agreements. At that time, there was a desire to obtain a new package of support aimed at developing cooperation in the defence sector. According to documents preserved by the National Archives of Romania (ANIC), our country had offered to assist in organizing the armed forces of the newly independent state and to provide political support for establishing a political regime similar to that functioning in Bucharest. To that end, Romania's Minister of Defence invited the future Chief of Staff of Zambia (Good, 1989, pp. 297-313)[4], Lieutenant Colonel Chinkuli Kingsley, to participate in a fact-finding visit. During discussions, the Zambian representative requested that our country should provide a significant package of military equipment, which was to include military aircraft. The delegation also included the Zambian Minister of the Interior, who was interested in how the youth movement in Romania was structured and operated. He also requested information regarding the training of agricultural specialists (ANIC, p. 15).

The cooperation between the two states strengthened over the following year, when, on 4 May 1971, the Zambian President expressed his gratitude for the support provided and invited a group of political consultants from the Romanian Communist Party to visit his country to participate in the activities of the United National Independence Party. It was hoped that they would present aspects of working in the field of economic security and participate in training the personnel responsible for countering disinformation (Ib., p. 39).

Motivated by fears of interference from British intelligence services in the political and economic functioning of the new state, Zambian representatives requested, among other things, the training of personnel specialized in counterintelligence. Thus, on 28 June 1971, President Kaunda requested Ceaușescu to prepare 6-10 specialists in Bucharest, who would operate in various structures responsible for national security. The goal was for the new officers to conduct activities against economic sabotage and to participate in combating fraud (customs, currency, and income tax). Additionally, there was a need to train future officers who would operate

[4] On 28 December 1970, Lieutenant Colonel Chinkuli Kingsley, aged just 31, was promoted to the rank of General and became the first indigenous Chief of Staff in Zambia. Despite the fact that he had been trained at the prestigious British Royal Military Academy Sandhurst (RMAS), during his military career he became one of the main supporters of national liberation movements in neighbouring states that followed the Zambian model and proclaimed their independence from the United Kingdom. (A.N.).

in military intelligence, capable of recruiting agents, conducting investigations, and interrogating suspects. There was also a requirement for training in technical areas specific to intelligence work, such as officers responsible for cryptography, secret writing codes, photography, and surveillance operations. During discussions, it was agreed that their training would take place in an intensive regime but would last no less than six months (Ib., p. 21). The agreement, signed on 23 November 1972, not only established the training in our country of the requested categories of intelligence officers but also foresaw an intensification of military intelligence cooperation between the two states. On that occasion, Romania created the opportunity to deploy intelligence officers in Africa (Ib., p. 118), which could provide a significant advantage over its economic competitors from both the socialist bloc and the West.

The political relations between the two states were strengthened in the following years, entering a new phase, in which the African leader communicated his main foreign policy decisions to Romania. One such moment was the communication of his key actions to support the national liberation movement in neighbouring Southern Rhodesia, which was still a British colony at the time. Through a telegram dated 23 March 1973, Kaunda informed Ceaușescu about the aggressive movements undertaken by the illegal regime (Nyerere, 1965, p. 373)[5] of Jan Smith, the leader of the white minority in the British colony of Southern Rhodesia. To provide additional details regarding the repeated violations of the state border and to request military support, the Zambian president sent two of his most important advisors, Mark Chana and Lishomma Lisshomwa, to Bucharest (ANIC, p. 72). They presented evidence of the aggression by the movement led by Jan Smith and its collaboration with the South African armed forces (ANIC, pp. 107-113)[6]. The first intervention of South African forces on the territory of Southern Rhodesia was recorded in 1967, when the South African police deployed over 2,000 members in support of the white minority, engaging in repressive actions against the native population (Moorcraft, McLaughlin, 2008, p. 32). To limit those incursions, which had already resulted in the deaths of 13 people, Zambia closed its state border starting on 9 January 1973,

[5] The province of South Rhodesia proclaimed its independence from Great Britain on 11 November 1965, under the leadership of the white minority that, at the time, represented only 5% of the region's population. The lack of legitimacy of the new regime, organized in a way similar to the Apartheid regime in South Africa, justified the movement to exclude the new state from the international community until 1980, when the native population, led by the future president Robert Mugabe, proclaimed the new African state called Zimbabwe. (A.N.).

[6] South Africa has repeatedly been accused of committing crimes against the civilian population, the apartheid regime being, in the opinion of President of Zambia, strongly supported by corporations active in the mining field: *"the political power of this regime was supported by international capital through multinational corporations".* The racist South African regime was branded by President Kaunda as fascist, and the fight against it described as a fight against *"colonialism, neo-colonialism racism and fascism".* He stated that independent Zambia has a *"historical duty and responsibility to support liberation movements".*

and abandoned supply routes transiting this region. This action significantly increased the costs of importing necessary products, which had to be transported via Dar es Salaam in Tanzania. In this context, the African president requested the delivery of port facilities, trucks, communication equipment, as well as financial support and technical training for personnel who would carry out supply activities through Tanzanian ports (ANIC, p. 74).

Another delicate moment in international relations was debated between representatives of the two states on 1 November 1973. Considering that Romania remained the only socialist state that, after the conclusion of the Yom Kippur War, still kept its embassy in Israel open, President Kaunda deemed it necessary to inform Bucharest about the suspension of relations between Zambia and Israel. The decision was motivated by the alleged expansionist tendencies exhibited by the Israeli state towards its neighbours. The actions undertaken by the Arab states during the Yom Kippur War were considered just and necessary to temper the aggressive tendencies of this state (Ib., p. 50). On that occasion, he informed Bucharest that his country would support the Palestinian people, but it should not affect the very good relations existing between the two states.

The military collaboration with Zambia extended throughout the 1970s, reaching a peak in the latter part of the decade when support for the Mugabe regime in the neighbouring country reached its highest levels. Following the visit of Alexander Grey Zulu, President of the Defence and Security Committee and Minister of National Defence, on 7 July 1979, important details were established for the continuation of the military cooperation between the two states. It was desired that Romania should continue to train Zambian military personnel, but reduce costs. Moreover, it was proposed that most of training activities should be conducted in their home country. The only accepted exception was the training of military personnel who would operate in commando units. During the visit of the Minister of the Interior, Wilted J. Phiri, on 6 September 1979, cooperation was extended to include the training of the Ministry of Interior's troops. The official requested the delivery of a significant military equipment package consisting of 30 armoured personnel carriers for police troops, 20 prison vans, 80 ARO cars, 2,600 automatic weapons with over 1 million cartridges, 200 machine guns with over 300,000 cartridges, 50 anti-aircraft artillery pieces with 100,000 rounds, and 64 mortars with 10,000 rounds (Ib., p. 102).

On 20 November 1982, the Minister of Legal Affairs and Attorney General of Zambia, Mr. Gibson Chigaga, arrived in Bucharest with the mission of examining the possibility of adopting the Romanian legal system. He aimed to analyse

the feasibility of amending the legal system inherited from the colonial era in his country to eliminate provisions that continued to *"protect capitalist interests"* (Ib., p. 126). Cooperation between Romania and Zambia reached its peak in the early 1980s, when our country became a potential model for organization and operation for the African state. This model was to be extended to neighbouring African states seeking rapid modernization.

ROMANIAN-ZIMBABWEAN MILITARY COOPERATION, AN IMPORTANT ELEMENT ON THE PATH TO POLITICAL INDEPENDENCE FOR THE AFRICAN STATE

Utilizing the experience gained during the 1970s in supporting Zambia's independence consolidation movement, Romania continued to provide new support packages to Southern Rhodesia (the future state of Zimbabwe), which was then engaged in its own struggle for independence. The Romanian state justified its military support to some of the newly independent African states as a necessary means to sustain the anti-imperialist struggle. This financial and military aid was provided at the request of leaders of guerrilla movements in Africa, such as Robert Mugabe. He invoked in support of his cause the fact that his adversary, Ian Smith, the leader of the white community in the former British province of Southern Rhodesia, received support from major powers. He argued that the assistance was delivered to white Rhodesians indirectly (ANIC, 3Z/1979, p. 5), without drawing attention to the blatant violation of UN directives, which recognized the national liberation movement of African states as just. The leader of ZANU (Zimbabwe African National Union) requested the Romanian state to provide a significant package of economic, financial, and especially military support.

Through a bilateral agreement approved by Nicolae Ceaușescu on 7 May 1978 (Ib., p. 3), the Romanian state committed to supplying the African state with weapons, financial assistance, and training for a large group of military personnel. In the initial phase, specifically in the three months following the signing of the agreement, Romania pledged to provide equipment and armaments for the rapid equipping of 6,000 soldiers. Additionally, it was to supply further materials for the training of new recruits who were to be enlisted from the populations of regions that were to be liberated. The most important part of the agreement stipulated that, during 1979, Romania was to host, equip, and train 2,000 African soldiers who were expected to arrive in our country as follows: 900 in the January-June period, 900 in the July-December period, and 200 were to be hosted by the Romanian state for a period of 3-4 years, necessary for their training as future officers specialized in artillery, aviation, and reconnaissance (Ib., p. 5).

Constrained by severe shortages, Mugabe requested that the Romanian side should approve financial support of $500,000, urgently needed to purchase essential food supplies to feed both the soldiers enlisted in his armed forces and the civilians in liberated areas. The funds were to be sent to ZANU through the Romanian embassy in Mozambique. He also requested the expedited delivery of medicines, transportation means, and either funds or parts necessary for maintenance. As for weaponry, Mugabe requested that the initial shipment should include 5,000 automatic weapons with 800 boxes of ammunition, 1,000 RPGs, 200 pieces of 82 mm mortars with 800 boxes of ammunition, 50 pieces of 120 mm mortars, 300 anti-aircraft machine guns of 12.7 mm calibre and 200 boxes of ammunition, 50 cannons of 75 mm calibre, 25 cannons of 85 mm calibre, 25 cannons of 107 mm calibre, 400 surface-to-air missiles, explosives, anti-personnel mines, chemicals, radios, and other military equipment (Ib., p. 8).

Another request from the Mugabe regime was that all the weapons and munitions should be shipped to Zimbabwe before the arrival of a group of 1,000 soldiers trained by the Ethiopian armed forces (Ndlovu-Gatsheni, 207, p. 63). The soldiers were part of a rival faction led by Joshua Nkomo, leader of the competing organization, ZAPU (Zimbabwe African Peoples Union). Despite ethnic differences (Msindo, 2012, p. 200)[7], which sooner or later could lead to armed conflict (Zhira) between the groups, the ZANU leader asked the Romanian state to make efforts to equip them. The request demonstrated the level of political maturity of the African regime, showing that it understood that the immediate goal shared by both groups was paramount. Achieving political independence from Great Britain and, above all, eliminating the white minority paramilitary group that sought to extend the Apartheid (Dubrow , 2014, p. 3)[8] regime into that region were the most important objectives to be achieved.

In the following year, Romania was asked to intensify efforts to train the soldiers sent by the African regime, given the limited capacity of the regime in Addis Ababa, Ethiopia, to increase the number of troops it was already training. At that time, Ethiopia was already involved in supporting Zimbabwe's independence struggle by training a significant number of soldiers, primarily recruited from the Nguni tribe.

[7] Mugabe belonged to the Shona ethnic group, a tribe associated with the Bantu population, the majority population in Southern Rhodesia, while his rival belonged to the Ndebele ethnic group, a tribe that is part of the Nguni-speaking peoples, who predominantly lived in South Africa.

[8] Apartheid was a slogan used by the white South African minority of Dutch descent (Boers) in the campaign aimed at proclaiming state independence from the British Empire. Later, the term was used to promote a regime of racial segregation established in South Africa between 1948 and 1994.

In a very short time, the Romanian side fulfilled its commitments to the African state. In February 1979, the military advisor and Chief of the Central General Staff of the Patriotic Guards, General Constantin Olteanu[9], reported to Nicolae Ceaușescu that the military aid worth 6,750,000 lei was loaded onto the ship *Tîrnăveni* and was expected to reach its destination within the same month. The next step in consolidating the relations between Romania and Zimbabwe was the reception of a delegation of ZANU members at the Ministry of Defence headquarters in Bucharest. During the visit, they established the necessary details for the arrival of the 1,000 soldiers in Romania, as well as the specifications regarding transportation costs. The amount of 35,160,000 lei was to be covered by Romania (ANIC, p. 20).

It is important to note that Romania contributed significantly to the development of Zimbabwe's national air defence structures. In Bucharest, the initial training requirements were established for future personnel who would operate in this field. The training program costs for the 200 soldiers who were to be integrated into the structures of Zimbabwe's future Air Force General Staff were estimated at over 200 million lei for just the first phase. Romania was set to train 10 pilots, 30 personnel specialized as aircrew, 10 aircraft mechanics, 100 anti-aircraft artillery operators, and 50 signal operators. The funds were to be allocated from the International Solidarity Fund of the CC of RCP (Ib., p. 21).

The development of military collaboration was just one component; the Romanian state also aimed to increase its involvement in the foreign policy actions of the new state by training future leadership cadres. To that end, it was decided that when the soldiers arrived for training, they would be accompanied by several political leaders. On the occasion of the delegation's arrival in Romania, the first diplomatic relations between the two states were also established. Among the delegation on the plane was Lovemore Mazivisa, the first representative of the African state in Romania.

Among those who visited Romania during that period was Deputy National Commissioner and Central Committee member of the ruling party, Josiah Tungamirai, who would later become the Chief of the Air Force (appointed to this role in 1982, right after returning from Romania, where he was trained as a pilot) (Ib., p. 25).

[9] General Constantin Olteanu was considered at that time one of Nicolae Ceaușescu's trusted men, who, starting in 1971, took on the task of removing a significant number of officers educated in the USSR from the active ranks of the Romanian armed forces, some of whom were active members of the Soviet intelligence service, the KGB. For his support, in March 1980, he was appointed Minister of National Defence, a position he held until December 1985, when he was appointed First Secretary and General Mayor of Bucharest. His last important position held until December 1989 was Secretary General of the Central Committee of the Romanian Communist Party (RCP) for foreign relations. (A.N.).

Another significant figure trained by the Romanian state was Mike (Rex) Tichafa, the military commander of Harare Metropolitan Province. Both officers subsequently held high-ranking positions in the military and political leadership of the new state.

It is worth noting that, at that time, Mugabe sought to secure a strong position not only against white colonists but also in relation to his African rivals, with whom he anticipated future conflicts after achieving state independence. For him, establishing a monopoly in collaboration with the Romanian state was a major imperative, as it could later ensure a steady flow of arms and ammunition, as well as a potential market for goods that could be exported despite any embargo the British might impose.

An important chapter in the collaboration between Romania and Zimbabwe remained the defence industry and the training of experts who would coordinate the new production capacities. To establish further details regarding the investments that Romania was to make, Ion Coman, Secretary of the Central Committee of the Romanian Communist Party (RCP) and member of the Executive Political Committee, was appointed to lead the negotiations.

The first phase involved a state visit by the President of Zimbabwe to Romania, allowing him to visit the location where young recruits from his country were being trained. In addition to the military camp in Cincu, Brașov County, where African soldiers were receiving training, President Canaan Banana also toured several industrial sites in the surrounding area (Ib., p. 3). It is important to mention that the Zimbabwean President acknowledged Romania's support, including in the political organization of his state. Despite the fact that the elections had been organized by the British, his organization, ZANU, had achieved a sweeping victory (Tevera, 1989, pp. 162-165). Romania advised the African state to continue fostering the relationships between the two political factions, ZANU and ZAPU, and to bring into the government white minority members who demonstrated an understanding of the new political context.

Despite winning the war, the leaders of Zimbabwe spoke of the extensive material destruction left behind and the urgent needs for resettling thousands of refugees, rebuilding destroyed farms, and even maintaining armed posts in certain areas to defend against any potential breach of national sovereignty (ANIC, 168/1980, p. 5). Collaboration with Romania was seen by Zimbabwean leaders as an opportunity to disapprove the *"imperialist and colonialist"* theory that economic development for the country was no longer possible from that point forward. Romania aimed to establish itself as a primary model for the empowerment of developing nations,

promoting the concept of *"peaceful coexistence"* with capitalist countries with which continued collaboration was encouraged. The sole exception to that approach was apartheid South Africa, led at the time by a racist regime (Ib., p. 10).

CONCLUSIONS

This chapter of our recent history has been very little analysed, and on the few occasions it has been discussed, unfortunately, only the economic shortcomings suffered by Romania have been brought into the spotlight. After years of investment in the economic, political, and military support of the new state, as expected, our country signed several contracts aimed at providing long-term loans for the development of various industrial sectors. Many of the new enterprises were to operate as joint ventures, with a significant portion of future profits being allocated to the Romanian state. The first investments were made in the mining sector, for which Romania exported machinery that was to be reimbursed through the extracted raw materials. Another important contribution to the development of this sector came from Romanian geological engineers who conducted prospecting and provided predictability for future investments. To accelerate the development of these enterprises, representatives of Romania expressed their willingness to cooperate even with privately-owned companies (Ib., p. 8).

Typically, these economic losses are specific to any period of market formation, and they are also experienced by major powers. It is interesting to note that former colonial powers declared that during the period they controlled these territories, their trade balance was heavily imbalanced, incurring considerable losses due to their inability to capitalize on the economic investments made there. It clearly indicates that, in the case of Romania, the results of the collaboration were expected to emerge later on. Unfortunately, after the collapse of the socialist system, which occurred at the end of the Cold War, Romania deliberately or because of its financial incapacity withdrew from most of the investments it had made in Africa, thus putting an end to an atypical episode in our national history.

BIBLIOGRAPHY:

1. Arhivele Naționale Istorice Centrale/National Historical Archives in Romania – ANIC, Collection C.C. al P.C.R., Secția Relații Externe/Foreign Relations Section, File 2Z/1970, p. 14, 15, 21, 39, 50, 72, 74, 102, 107-113, 118, 126; File 3Z/1979, p. 3, 5, 8, 20, 21, 25; File 168/1980, p. 5, 8, 10.
2. Brown, T. *Contestation, confusion and corruption: Market-based land reform in Zambia*. In Sandra Evers, Marja Spierenburg, Harry Wels, eds. (November 2005). *Competing Jurisdictions: Settling Land Claims in Africa*. Leiden: Brill Academic Publishers.

3. Darwin, J. (2021). *Visul imperial. Ascensiunea și căderea puterii globale 1400-2000*. București: Editura Litera.
4. Dubrow, S. (2014). *Apartheid 1948-1994*. Oxford University Press.
5. Frankopan, P. (2019). *Drumurile mătăsii. O nouă istorie a lumii*. București: Editura Trei.
6. Good, K. (1989). *Debt and the one-party state in Zambia*. In *The Journal of Modern African Studies*, 27.2.
7. Hlihor, Const. (2024). *Cu „mâinile altora". România și războaiele prin intermediari în Africa 1970-1985*. Cluj-Napoca: Editura Școala Ardeleană.
8. Melinescu, N. (2024). *Reporter TV în Africa în timpul Războiului Rece*. Oral history interviews, author's audio-video documents collection, apud Hlihor, Const. (2024). *Cu „ mâinile altora", op. cit.* point 7.
9. Moorcraft, P., McLaughlin, P. (2008). *The Rhodesia War. A military history*. Pennsylvania: Stackpole Books, Mechanicsburg, https://books.google.ro/books?id=oL-jaeM63P8C&printsec=frontcover&hl=ro&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false, retrieved on 20 October 2024.
10. Msindo, E. (2012). *Ethnicity in Zimbabwe. Transformations in Kalanga and Ndebele societies 1960-1990.* New York: University of Rochester Press.
11. Ndlovu-Gatsheni, S.J. (2017). *Joshua Mqabuko Nkomo of Zimbabwe: Politics, Power, and Memory*. Palgrave Macmillan.
12. Nyerere, J.K. (1965). *Rhodesia in the context of Southern Africa*. In *Foreign Affairs*, no. 44.
13. Shurmer-Smith, P. (2011). *Once the dust of Africa is in your blood: tracking Northern Rhodesia's white diaspora*. ACME: An International E-Journal for Critical Geographies, no. 10.
14. Stockwell, S.E. (2007). *The British Empire: Themes and Perspectives*. Blackwell Publishing.
15. Tevera, D.S. (1989). *Voting Patterns in Zimbabwe's Elections of 1980 and 1985*. In *Geography*, vol. 74, no. 2, JSTOR, http://www.jstor.org/stable/40571607, retrieved on 20 October 2024.
16. Tomlinson, B.R. (2003). *What Was the Third World?* In *Journal of Contemporary History*, nr. 2, http://www.jstor.org/stable/3180660, retrieved on 22 July 2024.
17. Zaayman, W.H. (2010). *Three Scrambles for Africa*. Czech Republic: Prague, https://dspace.cuni.cz/bitstream/handle/20.500.11956/35273/140025509.pdf?sequence=1&isAllowed=y, retrieved on 12 October 2024.
18. Zhira, M. *Uncovering the reality of state violence in Western Zimbabwe, 1982-1987*, https://journals.library.ualberta.ca/pi/index.php/pi/article/view/1440/978, retrieved on 24 September 2024.

POLITICAL-DIPLOMATIC REGROUPINGS AND MILITARY IMPLICATIONS AT THE BLACK SEA (FEBRUARY-OCTOBER 1939)

George-Daniel UNGUREANU, PhD
"General Grigore Constandache" Central Archive Depository, Pitești
DOI: 10.55535/RMT.2024.4.49

Generally speaking, the main events marking the development of international relations during the tumultuous year 1939, at least in Europe, were framed, chronologically, into March and April, respectively August and September. However, February 1939 saw the regular annual meeting of the Balkan Entente's Permanent Council (in Bucharest) and also the Soviet initiative for a "Black Sea Pact", while, in October, it was concluded the trilateral pact between Türkiye, Britain and France, immediately after the failure of the Soviet-Turkish discussions on a bilateral alliance pact. Meanwhile, several dramatic political and diplomatic changes had also taken place in this part of Europe, mainly as a result of the surprising German-Soviet rapprochement from August 1939. The main sources of the article consist of documents from Romanian military and diplomatic archives, supplemented by a series of historiographical contributions, quite diverse in origin and language.

Keywords: alliances; agreements; balance of power; intelligence; war;

INTRODUCTION

The events and developments that occurred during the dramatic year of 1939 have been, and continue to be, the subject of a huge number of historiographical contributions, for reasons that are more than obvious to anyone having some expertise in the field of history. When it comes to the question of chronological demarcations within the framework of this watershed year in European and world history, the vast majority of specialists in the field take as their reference points the total break-up of the Czechoslovak state in mid-March, followed by the renunciation by France and Great Britain of their policy of appeasement towards Germany, and then the initiation of contacts and, from 14 April, negotiations with the USSR, with a view to curbing German expansionism in Central Europe, German-Soviet contacts and negotiations (concluded with the signing of the Ribbentrop-Molotov Pact, in Moscow, on 23/24 August 1939), the outbreak of war in Europe (at the beginning of September), the defeat and division of Poland and, sometimes, the beginning of the *"Winter War"* between the USSR and Finland in late November.

The present article is atypical from this point of view, having as its main chronological landmarks two less dramatic calendar months of the year 1939, namely February and October. However, as far as we are concerned, we consider these months to have been of particular importance, taking into account the political, diplomatic and military developments in the Black Sea region. Thus, in early February 1939, in the context of a dinner hosted by the embassy of the Republic of Türkiye, the head of Soviet diplomacy, Maksim Maksimovich Litvinov, launched the idea of a *"Black Sea Pact"*, consisting of the USSR, Türkiye and Bulgaria, as an alternative to the Balkan Entente (Hitchens, 1983, p. 115), a regional alliance consisting of Romania, Türkiye, Greece and Yugoslavia. In the discussions at the Turkish embassy, Litvinov did not mention Romania, even though the Romanian state had a fairly large littoral area at the Black Sea. However, by the end of January, the Soviet side had already initiated a few inquiries about such a pact among the Romanian diplomats accredited in Moscow (Dobrinescu-Pătroiu, 1992, pp. 16-17). Between 20 and 22 February 1939, the regular annual meeting of the Balkan Entente's Permanent Council was held in Bucharest (I.P.E.R.D., 2003, pp. 309-310).

THE BLACK SEA COAST STATES IN EARLY 1939

The so-called *"Munich Agreement"*, finalized at the end of September 1938, marked the culmination of the appeasement policy followed by Great Britain and France towards Germany and the beginning of the break-up of the Czechoslovak Republic. That political-diplomatic act was also a moment of exclusion of the Soviet Union from the concert of European Great Powers, both by the London-Paris tandem and by the Berlin-Rome Axis (Kissinger, 2001, pp. 272-278). Europe's political and diplomatic scene was to be dominated by the arrangements in the Bavarian capital until mid-March 1939.

In the winter of 1938-1939, the Soviet Union, by far the most powerful state in the Black Sea region, seemed to be in a situation of isolation and weakness unprecedented after the 1918-1921 Civil War. Internally, the Stalinist purges had also affected the higher structures of the Red Army, and the Soviet state, ignored in the Munich arrangement, was also facing hostile military action in the Far East from Japan; as a solution, Stalin and some of his collaborators were increasingly considering a direct deal with Germany, some discreet signals being sent to Berlin (Ib., pp. 297-299; Constantiniu, 2010, pp. 85-86).

The impetuous development of heavy industry and the collaborations between the Soviet state and states or firms in the capitalist world also included or involved an important military dimension, a fact known, at least in general and in part, outside the Soviet Union, a situation that included Romania. Since, unlike pre-war Tsarist Russia, the inter-war Soviet state had only small access to the Baltic Sea, the commercial and military-strategic importance of the Black Sea and the coast of the Kola Peninsula had increased (Collection XIV, crt. 254/1939, l. 16). However, at the beginning of 1939, the intelligence services of the Romanian armed forces reported a *"feverish activity in all the shipyards"* of the Soviet Union, with three battleships and seven large cruisers under construction. The Soviet Union had no fewer than 160 submarines at its disposal, of which only *"a small fraction"* were deployed in the Black Sea, a situation that was attributed to other threats, namely the Japanese one in the Far East and the German one in the Baltic Sea (Ib., l. 23). At the same time, the Soviet political leaders and military commanders attached great importance to the development of aviation (Collection 5417, crt. 900/1939, passim). In Romanian military circles, the USSR's tendency to create strategic *glacises* (the word is used verbatim) had already been noticed, for the time being (only) in the Far East, with the Mongolian People's Republic and the Republic of Tuva being perceived in this way (Collection XIV, crt. 254/1939, pp. 18-19).

For Romania, the fundamental foreign policy objective at the beginning of 1939 remained that of preserving its territorial integrity, without, however, totally excluding the possibility of territorial concessions in Southern Dobruja (The *Quadrilateral*), a territory with a predominantly non-Romanian population, obtained from Bulgaria in the summer of 1913.

From a political-diplomatic point of view, under the conditions of the dissolution of the Czechoslovakian state (and implicitly, of the Little Entente), Romania maintained privileged relations with France, Great Britain, Poland and the allied states of the Balkan Entente, the Romanian legations in Paris, Ankara, Athens and Belgrade, yet not those in London and Warsaw, being raised to the rank of embassies in the winter of 1938-1939 (I.P.E.R.D., 2003, pp. 308-309).

The relations with Germany had undergone a crisis between 1938 and 1939, after the assassination of Corneliu Zelea Codreanu and other leaders of the Legion Movement by order of King Carol II, but pragmatism prevailed in both Bucharest and Berlin, and the diplomatic crisis was overcome in early February 1939. For the members of the government in Bucharest, Germany's need for raw materials (primarily grain and oil) was a solid premise not only for the development of bilateral trade, but also, by implication, to dissociate the *Reich* from Hungary and Bulgaria and to gain its interest into protect the borders of Greater Romania (Haynes, 2003, pp. 75-77). Consequently, talks on a bilateral economic treaty were initiated in February and finalized on 23 March (Ib., pp. 85-90).

The relations with the USSR were much more problematic and unpredictable, primarily because Moscow permanently avoided to explicitly recognize the unification of Bessarabia with Romania, *ipso facto* the common border along the Dniester. Bilateral trade opportunities were reduced, while the ideological factor also played a significant part. Bilateral diplomatic relations had been re-established in 1934, but after the recall of Mikhail S. Ostrovsky, followed by the flight of his interim replacement, Fyodor Butenko, to Italy (January-February 1938), the Soviet government had no longer appointed a plenipotentiary minister to Bucharest (Dobrinescu, 1991, pp. 116-117, 177).

Romania's mobilizable military potential in 1939 was, theoretically, about 3.5 million, representing a little more than one-sixth of the total population, but the mobilization documents actually listed only 1.55 million people, grouped into four armies or 11 corps. The experts in the Great General Staff's leadership estimated: *"There are human forces"*, yet *"for the time being, the lack of war material limits the number of large units that we can mobilize, although the needs would require an increase in the provisions of the current mobilization plan"* (*Istoria românilor/*

The History of Romanians, VIII, 2003, pp. 205-206). The Romanian naval forces included the Sea Division and the Danube Division, whose development was generally underfunded; in 1936 and 1939 new naval programs were developed and approved, but few of their provisions were materialized, and it was not until 23 May 1939 that the first Romanian submarine, *"Delfinul"*, was launched (Ib., p. 200).

The Turkish Republic had suffered the shock of losing its founding leader, Mustafa Kemal (*Atatürk*), on 10 November 1938. His place was taken by a close associate, Ismet Inönü, who remained President of the Republic for almost 12 years. On 25 January 1939, Mahmûd Celâl Bayar was replaced as Prime Minister by Refik Saydam (Popa-Matei, 2002, p. 534), and Şükrü Saracoğlu succeeded Tevfik Rüştü Aras at the head of Turkish diplomacy.

The area of the Republic of Türkiye in the early 1939 (before the acquisition of the Hatay/Alexandrette area, included after the First World War in French Syria) was 763,000 km^2, of which only 24,000 km^2 were in Europe, the so-called Eastern Thrace (Collection 5417, crt. 878/1939, p. 29). The population had reached almost 17.5 million, increasing by about a quarter within 12 years (Kyçyku, 2005, p. 95). The peace-time forces of the Turkish armed forces included about 10,000 officers, 20,000 non-commissioned officers and 150,000 troops (the equivalent of two contingents), while the mobilizable forces were estimated at a maximum of 1,200,000 (Collection 5417, crt. 878/1939, pp. 9-13).

On the political-diplomatic level, the Turkish state pursued a policy of balance between the Soviet Union (its great initial ally) and the Great Western Democracies (France and Great Britain), with which it had progressively improved its relations in the second inter-war decade, without however risking a deterioration of the ties with the USSR (Biagini, 2005, pp. 111-114). Türkiye firmly opposed the territorial revisionism promoted by Germany and Italy, but the Ankara regime's economic policy was more nuanced, with Germany accounting for 44% of Türkiye's exports and 11% of its imports in 1938 (Özden, 2013, p. 94).

Bulgaria, the smallest and most sparsely populated of the four Black Sea coast states, was not part of any regional alliance, promoting the so-called *"peaceful revisionism"*. Roughly 65% - 70% of Bulgaria's imports and exports went from, respectively to Germany, but Bulgaria accounted for only 2% of the *Reich*'s foreign trade. After Munich, hopes for peaceful territorial gains had grown exponentially, the most popular claim being Southern Dobruja, as Romania seemed to be the most isolated and vulnerable neighbour (Ungureanu, 2009, pp. 327-333).

With an area of 103,000 km^2 and almost 6,000,000 inhabitants, Bulgaria could theoretically mobilize about 750,000-800,000 men, but actually the trained troops that could be mobilized did not exceed 500,000. The Bulgarian armed forces included 14 infantry divisions, two rapid divisions, a mountain division and a Sea division. The latter division included two marine and two coastal artillery regiments. The two marine regiments were equipped, according to the information available to the Romanian General Staff, with four torpedo boats, six speed boats, three auxiliary vessels and one or two submarines, while the coastal artillery regiments included two divisions each, with 72 pieces of different calibre (Collection XIV, crt. 213/1939, passim).

From the military point of view, Romania, Türkiye and Bulgaria faced a number of similar problems and difficulties: the poor development of their own armaments industry and dependence on imports, the age and heterogeneity of their armaments, the low degree of motor mechanization etc., and from 1936 onwards, hasty and only partially successful efforts were made to remedy those shortcomings.

During the February 1939 meeting in Bucharest of the Balkan Entente's Permanent Council, the divergent trends within the alliance, which had been forged since 1936/1937, were again brought to the fore. Thus, Greece and Türkiye were in favour of strengthening collaboration with Great Britain and France, while Yugoslavia promoted an increasingly *"equidistant"* policy between the Great Powers, a policy that was actually favourable to the Berlin-Rome Axis, and the Romanian diplomacy tried to preserve the unity of the alliance. Bulgaria claimed, on the one hand, its readiness to join the alliance, on the condition of getting some territories, while, on the other hand, it tried to isolate Romania and Greece by developing ties with Yugoslavia and Türkiye (Ungureanu, ib., pp. 330-331).

In early 1939, Soviet-Turkish relations were good, as the gradual improvement in Türkiye's relations with Great Britain and France did not contradict the interests of the USSR, because of the caution of the Ankara government, and because the Soviet Union was still in the anti-revisionist camp. The precautions of Turkish diplomacy in relation to its large northern neighbour also manifested themselves within the Balkan Entente. The very founding document of this regional alliance, in its secret annex, noted Türkiye's unwillingness to get involved in a conflict with the USSR (I.P.E.R.D., 2003, p. 281), a reservation known in diplomatic circles as the *"Russian clause"*. However, the reservations categorically expressed in 1934 were to be partially diminished towards the end of 1937, when, in an official letter from Marshal Fevzi Çakmak, the Turkish state undertook to act against Bulgaria in the event of a joint Soviet-Bulgarian attack on Romania (Ib., p. 302).

The content of the discussion between M.M. Litvinov and the Romanian minister in Moscow, Nicolae Dianu, on 8 February 1939, is very relevant for the specifics of Romanian-Soviet relations in the first half of 1939. According to the Romanian diplomat, Litvinov began his exposition by criticizing Great Britain's and France's passivity in relation to Germany, pointing out at the same time that the USSR had received and rejected a series of proposals for economic collaboration from Berlin. Litvinov went on to refer to the breaking of diplomatic relations with Horthyist Hungary as a result of the latter's adherence to the Antikomintern Pact, described as *"a pact of aggressors"*, directed primarily against France and Great Britain (!), and towards the end he sought to minimize, in the eyes of the Romanian interlocutor, the danger of Bulgarian revisionism and especially the significance of certain references to Bessarabia in the local Soviet press, namely the non-appointment of a plenipotentiary minister in Bucharest (M.F.A.R.- M.F.A.R.F., 2003, doc. 102, pp. 220-222).

Soviet-Bulgarian relations had just begun to improve and amplify, from an economic, cultural, journalistic and propaganda standpoint, and that trend was noted by the Romanian military-information structures, which also noted the r e-establishment of collaboration between Bulgarian right-wing (nationalist) and left-wing subversive organizations in Dobruja (Collection 950, crt. 651/1938, pp. 46-47; Ib., crt. 227/1939, pp. 159-160); moreover, the Bulgarian diplomatic research conducted in Moscow on the "*Dobrujan question"* in November 1938 and January 1939 had ended with encouraging results (Ungureanu, p. 330).

Encouraged by the general European climate increasingly favourable to territorial revisionism, the rulers in Sofia practically abandoned the direct negotiations with Romania, initiated in 1933, in order to conclude a bilateral treaty on the basis of the existing borders; the method used was that of postponement *sine die*, combined with the reopening of previously agreed issues (Ib., pp. 332-333).

At the time, Turkish-Bulgarian relations were dominated by Turkish diplomatic efforts to bring Bulgaria into the Balkan Entente and, at the same time, strained by tensions due to the Bulgarian authorities' treatment of the country's Turkish-Muslim minority, representing about one tenth of the total population, or, in absolute figures, about 600,000 people (Stănciugel, 2008, p. 171).

In the first half of February 1939, the Yugoslav government of Milan Stojadinović was replaced with a government led by Dragiša Cvetković. This act of Prince Regent Paul (*Pavle*, in Serbian) was based on both domestic and foreign reasons, as he did not agree with Yugoslavia's sliding into the Berlin-Rome Axis (Jelavich, 2000,

pp. 187, 197), which was also known in certain Romanian military-intelligence circles (Collection 950, crt. 201/1938, p. 157).

At the annual meeting of the Balkan Entente's Permanent Council (Bucharest, 20-22 February 1939), some different attitudes towards Bulgarian territorial claims were also manifested. On the eve of the meeting, Georgy Kiosseivanov, the head of the government in Sofia and also head of Bulgarian diplomacy, had tried to convince Ş. Saracoğlu of the justness and advisability of ceding South Dobruja as a *sine qua non* condition for Bulgaria's joining Balkan Entente, gesture desired in Ankara, but in Bucharest, Grigore Gafencu and Ioannis Metaxas (head of the Greek government) firmly opposed to any territorial concessions, and claimed for regional cooperation on the basis of the existing borders (Ungureanu, p. 331). After the signing of the Bulgarian-Yugoslav pact of *"eternal friendship"* on 24 January 1937, Bulgarian revisionism was channelled towards Greece and Romania.

THE LAST PEACEFUL MONTHS (MARCH-AUGUST 1939)

The dissolution of the Czechoslovak statehood in mid-March 1939 by Nazi Germany, with the assistance of Slovak nationalists and Horthyist Hungary, despite all previous assurances, prompted Britain and France to abandon their policy of appeasement and to take diplomatic steps to build a broad anti-revisionist front in Central and South-Eastern Europe, including Soviet Union. These political-diplomatic projects and approaches, with important military implications, dominated the European scene until the Ribbentrop-Molotov Pact was concluded, which effectively signalled the outbreak of war in Europe.

The dramatic political-territorial developments in the immediate vicinity of Romania, chronologically superimposed on the last stages of the negotiations for the Romanian-German economic treaty, generated a tense atmosphere in Romania; in that context, the mobilization of several contingents was decreed and rumours were spread about an ultimatum given by the Reich to the government in Bucharest, in order to quickly conclude the bilateral economic treaty (the famous *"Tilea incident"*).

On the very day of 17 March 1939, Virgil Viorel Tilea, Romania's minister in London, had a discussion with the Turkish representative in the British Capital, the former foreign minister Tevfik Rüştü Aras. The Turkish diplomat spoke strongly in favour of building a Black Sea Pact and of the Balkan Entente's consolidation, being firmly convinced that the Soviet Union was really interested in blocking German expansion (Dobrinescu-Pătroiu, 1992, p. 28). The next day, the Romanian military attaché in Ankara, Lieutenant-Colonel Traian Teodorescu, indicated in a report

that both Turkish rulers and public opinion wanted to transform the Balkan Entente into a *"foreign political entity with broader aims than it has at present"* (Collection 5417, crt. 830/1939, pp. 29-30). For the Turkish diplomacy, therefore, the Black Sea Pact project did not contradict the objective of consolidating the Balkan Entente; instead, it was complementary to it, unlike the early February initial Soviet proposal.

On 17-19 March 1939, G. Kyosseivanov paid an official visit to Türkiye. In this context, as multiple military and diplomatic sources record, the Turkish dignitaries manifested, in the clearest and most categorical manner, their determination to respect their obligations as a regional ally of Romania, in case of a Bulgarian attack on Romania, regardless of other hypothetical circumstances, successively evoked by Kyosseivanov: the involvement of Hungary and Germany, the passivity of the other Balkan allies etc. (Ungureanu, p. 332). Military Attaché Teodorescu sent a report on this subject on 22 March 1939 (Collection 5417, crt. 830, pp. 9-12). In a discussion with Lieutenant-Colonel Teodorescu, the Chief of the Turkish Army General Staff, Field Marshal Fevzi Çakmak, assured his interlocutor that Türkiye had sufficient forces to neutralize Bulgaria, even in the event of an Italian attack in the Izmir region (Ib., pp. 15-16). Moreover, on 22 March 1939, the Romanian military attaché in Ankara also reported that he had received assurances from the Soviet ambassador, Aleksei V. Terentiev *("If Romania holds its position firmly, Russia will supply it with everything it needs")*, expressing, at the same time, his surprise and suspicion at the attitude of Soviet diplomats in Türkiye towards their Romanian counterparts, which he considered *"overly courteous"* (Ib., pp. 16-17).

The next day, the Romanian-German economic treaty was concluded. The event was hailed in Berlin and Rome, criticized in London, Paris and Moscow, yet it aroused consternation in Budapest and Sofia (Dobrinescu-Pătroiu-Nicolescu, 1999, pp. 226-227), which confirmed, at least temporarily and partially, the correctness of some political-diplomatic calculations of the leaders in Bucharest.

On 29 March 1939, through the voice of M.M. Litvinov, the Soviet government expressed to the Romanian diplomat Nicolae Dianu not only its dissatisfaction, but also some suspicions about the content and significance of the Romanian-German economic treaty, including certain alleged secret clauses of the agreement, which, in the Soviet view, were likely to turn Romania into a base for German expansionism at the Black Sea. The head of Soviet diplomacy linked the act performed on 23 March 1939 to certain *"anti-Soviet"* positions in Romania, and reiterated his well-known position on the futility and inappropriateness of an official Soviet declaration explicitly recognizing Romania's sovereignty over Bessarabia (M.F.A.R.-M.F.A.R.F., 2003, doc. 107, pp. 227-228).

On 8-9 April 1939, Romanian Foreign Minister Grigore Gafencu paid a visit to Ankara, where he had talks with his Turkish counterpart, Şükrü Saracoğlu (I.P.E.R.D., 2003, pp. 312-313). The diplomatic moment was commented favourably by the Soviet press agency TASS, probably on the basis of information from the USSR's chargé d'affaires in Bucharest, Pavel G. Kukoliev (Collection 5417, crt. 830/1939, pp. 2-4).

An even more important diplomatic moment took place on 13 April 1939, when France and Great Britain simultaneously announced the unilateral granting of solemn guarantees of independence to Romania and Greece (I.P.E.R.D., 2003, p. 313). That act had rather a moral value and showed, at least in the case of Romania, a half-committal attitude on both sides: France and Great Britain avoided explicitly guaranteeing Romania's territorial integrity, thus keeping a certain margin of negotiation with Hungary, Bulgaria and especially the USSR, while Romania, for its part, avoided taking a very categorical stance in favour of the two guarantor powers, in order not to break, at least for the time being, all bridges with Germany, seen as a counterweight to the USSR.

On 14 April 1939, the tripartite Franco-British-Soviet talks began in Moscow, and lasted more than four months, without any concrete result. Mutual suspicions and diverging visions and interests were to prove stronger than the potential factors for rapprochement.

A number of issues concerning the Central and Eastern European states situated between Germany and the USSR, which were reluctant towards the Bolshevik great power, but subject to demands and conditions made by the Soviet side to the French and British negotiators, proved insurmountable. In the summer of 1939, in all these small and medium-sized states, the Soviet proposal for France and Great Britain, to include in the future tripartite agreement the phrase *"indirect aggression"*, defined as a domestic political change to the advantage of the aggressor, caused great anxiety, because it opened up wide possibilities for interference in the internal affairs (Kissinger, 2001, p. 305; Constantiniu, 2010, pp. 86-87).

At the regional level, for the second half of April 1939, one can also note certain dissatisfaction on the Turkish side, through Şükrü Saracoğlu, with the attitude of Romanian diplomacy, which was considered too intransigent in the South Dobruja issue (Stănciugel, p. 175). However, in March-April 1939, the ruling circles in Bucharest were considering the option of partially ceding the *Quadrilateral*, but only on the condition that Bulgaria would join the Balkan Entente or a system of alliances close to Great Britain and France (Ungureanu, pp. 332-335).

Bulgarian demands were, however, larger, and Bulgarian availability, much smaller. Thus, on 19 April 1939, Georgy Kyosseivanov sent to all Bulgarian diplomatic missions the six-point Directive No. 19 on Bulgaria's position, conduct and aims in the general European context of the time. According to this document, Bulgaria's minimal territorial claims were South Dobruja and Western Thrace, and the readiness for integration into a regional alliance system was almost null (I.I.D., 1993, part II, doc. 44, pp. 358-359).

From 26 April to 8 May 1939, Vladimir Petrovich Potëmkin, one of the deputies of the Soviet chief diplomat, took a regional tour, including Romania, Bulgaria, Türkiye and back, namely the states bordering the Black Sea. A few days before the beginning of that tour, V.P. Potëmkin had a meeting with Nicolae Dianu, during which he emphasized the strategic importance of Romania and Türkiye for the security of the south-western borders of the Soviet Union (Dobrinescu-Pătroiu, 1992, p. 70).

During his journey through Romania to Sofia, in Bulgaria, the Soviet dignitary was not invited to talks with any high Romanian official, in order not to upset Germany (Haynes, 2003, p. 109). The desire not to provoke Germany was also the explanation offered by Grigore Gafencu to his French interlocutors at the end of April 1939, during his visit to Paris, when he was questioned about Romania's reluctance towards the Soviet Union (Dobrinescu-Pătroiu, pp. 76-77).

In early May, Romania's ambassador to Türkiye, Vasile Stoica, also received suggestions from Ș. Saracoğlu to improve Romanian-Soviet relations. The head of Turkish diplomacy sought to demonstrate to Ambassador Stoica the lack of viability of the anti-revisionist plans involving Central and South-East Europe, in the absence of at least passive cooperation (benevolent neutrality) on the part of the USSR (Stănciugel, p. 187). The President of the Republic of Türkiye, Ismet Inönü, went even further with his political-military reasoning, arguing, in discussions with French and British interlocutors, that, in the event of war, the Red Army should be directly and massively involved against Germany, so as not to give the Soviet Union the chance to remain neutral and to take advantage of the mutual exhaustion of combatants, in order to expand its social-political regime in Europe (Ib.)

It was also in early May, upon his arrival in Ankara, that Potëmkin had a meeting with the French ambassador to Türkiye, R. Massigli, that the Soviet diplomatic official hinted that there was a possibility that the USSR would issue an official statement on the renunciation of any claims to Bessarabia; the information was communicated by the French diplomat to Vasile Stoica, and was transmitted

to Bucharest on 17 May 1939 (Dobrinescu-Pătroiu, p. 93, note 100). During his discussion with his French counterpart, V. Stoica, taking note of that piece of information, told that such a categorical unilateral declaration could only have a positive effect on the Romanian-Soviet relations, while pointing out that, from a strictly legal point of view, Romania did not need such an act from the Soviets (Stănciugel, p. 176).

However, in his direct discussion with Vasile Stoica on 3 May 1939, Potëmkin did not address this issue, but summarized his talks in Sofia with Georgy Kyosseivanov, who had again tried to justify Bulgaria's non-adherence to the Balkan Entente by blaming Romania's intransigence on Southern Dobruja (Ib.). The Soviet dignitary then questioned the Romanian diplomat about Romania's readiness to join the USSR and other states *"in a broad anti-revisionist front".* In his answer, Stoica showed Romania's willingness to defend its borders and to contribute to the defence of peace and the territorial *statu quo* in Central and South-Eastern Europe, on the basis of the country's existing alliances; the idea of Romania's joining new alliances was not totally excluded, but was considered worthy of consideration (only) in the event of imminent or actual aggression against the Romanian state (Ib., pp. 187-188). Basically, Stoica reiterated, in a rather convoluted and polite form, the vision of the Bucharest rulers, who invoked the risk of unnecessarily provoking Germany as a reason for their reluctance to various regional projects involving the Soviet Union.

On 3 May 1939, newly installed at the helm of Soviet diplomacy, Vyacheslav M. Molotov, sent to V. P. Potëmkin one of his first telegrams in his new capacity. The telegram contained an outline of a plan for regional cooperation and two recommendations for the Ankara-Sofia-Bucharest return route. Thus, Bulgaria was to be included in the *"common front against aggressors"*, an objective for which Türkiye was to put pressure on Romania to cede Southern Dobruja. At the same time, Potëmkin was advised to return directly to Moscow, possibly with a short stopover in Sofia, in order to address his hosts with *"a few warm words, which do not oblige to anything".* Towards Romania, the attitude should have been even more reserved: *"We advise you not to stop in Romania, and if the Romanians nevertheless board your carriage, you can talk to them about weather"* (Sturza, 2016, pp. 202-203).

Not coincidentally, Potëmkin's telegram to Molotov, sent from Bucharest on 8 May 1939, a letter rather brief, began with the self-justifying phrase *"I could not avoid the meeting with Gafencu"* and focused on the reservations and dissatisfactions expressed in the discussion with the Romanian Foreign Minister (Ib., p. 203).

The head of Romanian diplomacy gave a somewhat more extensive description of the meeting. In contrast to his Soviet interlocutor, Gafencu recorded, first, Potëmkin's assurances that replacing Litvinov as head of Soviet diplomacy did not mean changing the foreign policy guidelines of the USSR, and finally, his interlocutor's promise of the imminent appointment of a plenipotentiary minister in Bucharest. Gafencu attributed to Potëmkin the conclusion that any concessions, especially territorial ones, towards Bulgaria, were inappropriate. As far as the exchange of opinions on the Romanian-Polish military alliance is concerned, the two accounts are convergent, at least *grosso modo*, as it is the avoidance by both diplomats of any direct reference to delicate issues in bilateral relations, such as Bessarabia or the possibility of concluding an alliance treaty (M.F.A.R.-M.F.A.R.F., 2003, doc. 112, pp. 234-235).

The exclusively anti-Soviet character of the conventions subsumed under the Romanian-Polish military defence alliance was not likely to please Potëmkin, but Gafencu assured him that there were both the possibility and the intention to turn the alliance into an *erga omnes* one, which was not to happen, however, due to the reluctance of the Polish side, which invoked the need not to provoke Germany (Dobrinescu-Pătroiu, p. 71). A month later, N. Dianu characterized Potëmkin's attitude towards Romania as *"cold"* (Ib., pp. 107, 116), in flagrant contradiction with the image left to posterity by G. Gafencu in his memoirs (Gafencu, 1992, pp. 187-190).

The signing of the Turkish-British declaration (12 May 1939) and the Turkish-French one (23 June 1939) marked a new stage of political-diplomatic developments in South-East Europe. Unlike the guarantees given to Romania and Greece on 13 April, those acts were bilateral in nature and presupposed a committed attitude on the part of Türkiye (Cojocaru, 2014, pp. 195-201). Of the member states of the Balkan Entente, Türkiye felt the least pressure from Germany and turned, more and more transparently, towards Great Britain and France, which were just negotiating an agreement with USSR, its old ally.

In the light of those geopolitical and diplomatic coordinates, we can understand the disapproving reaction of Turkish decision-makers to the Romanian-German economic treaty of 23 March 1939, which was considered, in the days immediately preceding 12 May 1939, as *"detrimental to Romania's interests"* (Collection 71/ Türkiye 1920-1944, vol. 61, pp. 108-109). Actually, immediately after the signing of the Turkish-British bilateral security declaration of 12 May, Germany's share in Türkiye's foreign trade halved (Özden, 2013, p. 94).

Romania's more cautious conduct towards Germany was also manifested during Grigore Gafencu's visit to Ankara on 11-14 June 1939, only nine weeks after the previous one, when the head of Romanian diplomacy obtained from his Turkish counterpart the promise that the Balkan area would not be mentioned in the text of the final Anglo-French-Turkish treaty (I.P.E.R.D., 2003, p. 316). In the same context, Gafencu rejected Saracoğlu's suggestions, which were probably inspired by the Soviets, concerning Romania's accession to the Black Sea Pact and the ceding of Southern Dobruja in order to draw Bulgaria into the Balkan Entente, pointing out that the Romanian state could not precipitately change its attitude towards Germany or the USSR, and that the government in Sofia were not really interested in adhering to the Balkan Entente (Dobrinescu-Pătroiu, pp. 103-104). According to a telegram sent by Gafencu to the Romanian minister in Warsaw, R. Franasovici, Saracoğlu insisted on the Black Sea Pact, making it known that Türkiye intended to conclude a treaty of alliance with the USSR; in the end, the two foreign ministers agreed that Türkiye would mediate between Romania and USSR, and Romania, between Türkiye and Poland (Collection 71/ Türkiye 1920-1944, vol. 61, l. 169).

Also in the middle of June 1939, as Soviet and German sources prove, Bulgarian diplomacy, through the minister in Berlin, Purvan Draganov, sought to strengthen the tendencies of rapprochement between Germany and the USSR, already noticed in certain circles. According to the diary of Georgy Astakhov, the USSR's chargé d'affaires in Germany, and to a memorandum drawn up by Ernst Woermann (one of Joachim von Ribbentrop's deputies), in separate talks with the two diplomats, on 14 and 15 June 1939, Draganov had mentioned in favourable terms the possibility of a direct and comprehensive German-Soviet agreement, considered to be advantageous not only for the two Great Powers, but also for Bulgaria, in order to gain territorial advantages. In that context, the Bulgarian diplomat had mentioned, during both meetings, Southern Dobruja, and, in the first discussion, the access to the Aegean Sea, blaming France and Great Britain (Sturza, 2016, pp. 205-207).

At the end of June and the beginning of July 1939, the Romanian-Soviet relations saw difficult moments. Thus, on 28 June, on V.M. Molotov's orders, his deputy, V.P. Potëmkin, summoned the Romanian minister in Moscow, N. Dianu, to inform him in very categorical terms of the Soviet government's dissatisfaction with the use, in a note addressed by the Romanian Legation to the Soviet side, of the expression *"Romanian territory"*, referring to a place in Bessarabia. Such a thing was considered unacceptable by the Soviet officials and had been communicated as such to the Romanian side as early as June 1938 and taken into consideration

by the Romanian side during the following year. Consequently, the note of the Romanian Legation was returned as unacceptably worded, which was a veritable diplomatic incident (M.F.A.R.–M.F.A.R.F., 2013, doc. 114, pp. 237-238). A week later, Dianu sent a telegram to Bucharest, at the end of which he noted that the Soviets had resumed *"the system of chicanery and blackmail concerning the Bessarabian question".* According to the Romanian diplomat, one of the reasons for that development was Romania's refusal to categorically and unconditionally accept the Soviet Union's guarantees and aid, as well as Romania's reluctance to accept the Black Sea Pact (Dobrinescu-Pătroiu, pp. 117, 127).

On 8 July 1939, King Carol II discussed with G. Gafencu the international situation, especially the Soviet insistence on the *"indirect aggression"* clause in the negotiations with the French and the British; the resumption of the Soviet press campaign on Bessarabia was also discussed. The king asked the head of Romanian diplomacy to communicate to London, Paris and Ankara Romania's concern over *"the Soviet claim to guarantee countries, even without their will, when the USSR believes they are in danger"* (Ib., pp. 118-123).

The older topic of Romania's possible joining the Black Sea Pact was approached on 10 July, in a discussion between Vasile Stoica and Şükrü Saracoğlu. The Romanian ambassador in Ankara was in favour of the idea of Romania's accepting the Pact in exchange for a non-explicit, (apparently) spontaneous and unilateral official declaration by the USSR, in the sense of explicit recognition of Bessarabia's belonging to Romania (Stănciugel, p. 177). A few days later, however, the head of Romanian diplomacy, Grigore Gafencu, sent a circular telegram in which, reminding the complexity of the international situation, he cited arguments for the lack of interest in the Black Sea Pact, but also the abstention from protests and other gestures, in reaction to the press campaign in the USSR regarding Bessarabia. In another telegram, addressed to V. Stoica, on 14 July 1939, G. Gafencu rejected the idea of joining the Black Sea Pact, even in the event of the USSR recognizing the common border along the Dniester (Ungureanu, p. 337).

An important discussion on the international situation took place on 26 July 1939 between King Carol II, Prime Minister Armand Călinescu and Foreign Minister Grigore Gafencu, in which the King considered Türkiye as Romania's most loyal ally, and Hungary and Bulgaria as effectively placed in the camp of the Axis Powers. Türkiye was also seen as a viable intermediary in the difficult relations with the USSR, and the Romanian sovereign hoped to conclude a bilateral non-aggression pact, recognizing the common border at the Dniester. In the undesirable eventuality

of Soviet troops landing in Bulgaria, in the context of a hypothetical, but increasingly probable war, the Turkish troops were, in Carol II's vision, to position themselves between the Romanian military units and the Red Army forces, in order to prevent direct contact between them (Călinescu, 1990, pp. 420-421).

At the end of July 1939 and at the beginning of the following month, a Bulgarian parliamentary delegation visited the USSR. According to an Italian source, during the discussions with the members of the delegation, V.M. Molotov expressed sympathy for Bulgarian claims on Dobruja, but avoided commenting on the question of Bulgaria's access to the Aegean Sea, and made concrete proposals for increasing bilateral trade (I.I.D., 1993, part two, doc. 48, pp. 368-369). At the same time, on 4 August, Soviet General Boris Shaposhnikov (future Marshal) wrote down some considerations on the progress of the tripartite military negotiations with Great Britain and France. General Shaposhnikov considered it necessary, among other things, to ensure a passage for Red Army troops through Romania to counter possible German-Hungarian-Bulgarian aggression. Also, in case of Bulgaria's involvement in the war on the side of the unnamed *"main aggressor"* (Germany – our note), France and Great Britain would have to draw Greece and Türkiye into the war, on the opposite side (Sturza, 2016, p. 211).

On 11 August 1939, the third Romanian-Turkish high-level political-diplomatic contact in four months took place. That time, the two authoritarian heads of state, Carol II and Ismet Inönü, met. The Republic of Türkiye was determined to defend the territorial *status quo*.

The Romanian monarch and the Turkish president agreed to step up their démarches in Belgrade and their ties with Poland. With regard to the USSR and the position of its large Eastern neighbour towards Romania, the Turkish side undertook to carry out certain diplomatic research actions, but reiterated the suggestion that Romania should join the Black Sea Pact, otherwise the chances of obtaining certain concessions from the Soviets were considered minimal (Collection 71/Türkiye 1920-1944, vol. 61, pp. 189-204). The refusal to join the Black Sea Pact was motivated by the Romanian side, that time as well, on the grounds that such a gesture would have represented a provocation towards Germany (Dobrinescu-Pătroiu, p. 134). On 13 August 1939, Carol II once again presented A. Călinescu his vision of Romanian-Turkish-Soviet relations: *"If the Soviet Union formally recognizes Bessarabia, we will then be able to move to a non-aggression pact, Saracoğlu will test in Moscow. Any Black Sea Pact is out of the question"* (Călinescu, p. 424). On the same day, the man who had officially taken the presidency of the Romanian

Council of Ministers five months earlier, noted in his diary: *"General D. Popescu and Colonel Paul Leonida are returning from Ankara, Türkiye, with very good results, they will bring 200 battalions to Thrace and their objective is to put Bulgaria out of fighting"* (Ib., p. 424). Thus, on 15-21 August, synchronized Romanian and Turkish military manoeuvres took place near Bulgaria's borders, in order to deter a possible aggressive action (Stănciugel, p. 199).

At the European level, however, things began to take a turn that few had anticipated a few months earlier. German-Soviet contacts suddenly intensified in mid-August, and on 23 August 1939, German Foreign Minister, Joachim von Ribbentrop, arrived in Moscow, by which time a bilateral German-Soviet economic agreement had already been concluded. By concluding a number of German-Soviet political deals, Hitler removed (at least temporarily) the possibility of confronting formidable adversaries (Great Powers) on two fronts, while Stalin succeeded, on the one hand, in precipitating a war between the capitalist Great Powers and, on the other hand, in gaining the opportunity to create a strategic *glacis* on the western borders of the USSR (Constantiniu, 2010, pp. 88-93).

In the German-Soviet talks of 23 August 1939, Türkiye was also mentioned; it was accused of having adhered to the policy of encircling Germany (Ribbentrop), or, as Stalin put it, of vacillations and duplicity (Hitchens, 1983, p. 216). Hitler's aim with Türkiye was to stop its rapprochement with France and Great Britain and to bring it to a policy of equidistant neutrality, yet he did not agree with its entry into the Soviet influence (Ib., pp. 206, 223).

FROM THE RIBBENTROP-MOLOTOV PACT TO THE ANGLO-FRENCH-TURKISH PACT (AUGUST-OCTOBER 1939)

On 23/24 August 1939, in Moscow, after several hours of discussions with Stalin, Ribbentrop signed a bilateral *"non-aggression pact"* with Molotov, which also contained a secret additional protocol concerning the delimitation of the spheres of influence between the two totalitarian Great Powers, from the Baltic to the Black Sea. While the delimitation was rigorous in the Baltic area and the Polish territories, the same cannot be said for South-Eastern Europe (I.P.E.R.D., 2003, p. 317; Sturza, 2016, pp. 224-225).

The conclusion of the August 1939 German-Soviet economic and political agreements came as a major surprise to many political and military decision-makers, who had based a number of calculations, hypotheses and projects on the idea that the contradictions between Germany and the USSR were irreconcilable.

On 22 August 1939, Armand Călinescu wrote in his diary: *"the coup de théâtre of the German-Soviet agreement"*, asking rhetorically, *"Did they agree on the division of Poland and Romania?"* (Călinescu, p. 425). The next day, the Romanian prime minister recorded his conviction that, despite the German-Soviet rapprochement, *"England, France, Poland and Türkiye will go ahead"* (Ib.). The establishment of a German-Soviet economic partnership significantly reduced Romania's room for manoeuvre in its relations with Germany.

The news of the Ribbentrop-Molotov pact also shocked the head of Turkish diplomacy, Şükrü Saracoğlu, who characterized it as *"a coup de théâtre unheard of in history"*; in the new context, negotiations for a Turkish-Soviet alliance treaty were becoming complicated (Hitchens, pp. 227-228) However, the Turkish foreign minister correctly assessed that his country had not been abandoned by Germany in the Soviet sphere of influence; on 27 August Türkiye rejected the *Reich*'s economic proposals (Ib., pp. 231-232).

In Bulgaria, the turning point in German-Soviet relations was received with satisfaction and enthusiasm, as the pact of 23 August 1939 united the most popular Great Powers in Bulgarian public opinion (Ungureanu, pp. 342-343). On 25 August 1939, the Romanian diplomat Nicolae Florescu, deputy director at the Ministry of Foreign Affairs, sent a telegram from London to the minister in charge, Grigore Gafencu, citing information received from *"fellow diplomats in the Balkan Entente states",* according to which, encouraged by the Soviets, the Bulgarian authorities had intensified pan-Slavism propaganda abroad (M.F.A.R.–M.F.A.R.F., 2003, doc. 117, p. 244).

On 1 September 1939, Nazi Germany's aggression against Poland began, and two days later Great Britain and France declared war on the aggressor Germany. The Second World War thus broke out in Europe. As early as 3 September 1939, the Romanian government intervened with the Turkish government and obtained its consent to supply the Polish armed forces with war material through the Straits, *via* Romania (I.P.E.R.D., 2003, p. 318). At that time, Poland was still expected to resist for a long time, and a war of positions was expected. After only two weeks, the supply route for the Polish armed forces would turn into a corridor of refuge for many Polish dignitaries, soldiers and civilians.

On 4 September, in a discussion with V.G. Dekanozov, one of Molotov's deputies in the Soviet diplomatic leadership, N. Antonov, the Bulgarian minister in Moscow, expressed the satisfaction of the Bulgarian government and people with the improvement in German-Soviet relations, and in this context expressed the hope that the USSR would help Bulgaria in the *"Dobruja question"* (Sturza, p. 236).

At the same time, German diplomats insisted with V.M. Molotov that the government in Moscow intervene with the government in Ankara so that Türkiye would maintain strict neutrality; the Germans were alarmed by rumours of French and British military forces crossing the Straits to land in Romania (Ib., p. 237).

At the Crown Council of 6 September 1939, which confirmed Romania's neutrality, King Carol II mentioned the possibility of Türkiye brokering a détente in Soviet-Romanian relations (Mamina, 1997, p. 182). According to Armand Călinescu's notes, during the discussions, Constantin Argetoianu raised the issue of relations with the Soviet Union *("Russia")*; the monarch replied that diplomatic action had already been initiated in this regard, through Türkiye (Călinescu, p. 430).

On 17 September, when the collapse of Poland was imminent and the Red Army had entered the territories east of the Curzon Line, Armand Călinescu inserted two proposals in his diary, both of which implied a certain role for Türkiye, namely a non-aggression pact with the USSR and drawing Bulgaria into the Balkan Entente, even on the condition of satisfying certain of its territorial claims (Ib., p. 432). Surprisingly, a ray of hope seemed to come from Moscow itself. The official Soviet communiqué on the entry of Red Army units into the territory of the dissolving Polish state contained the periphrasis *"the Dniester River, which is our border with Romania"*, a fact also noted by N. Dianu (Lungu-Negreanu, 2000, doc. 19, p. 188).

On 17 and 18 September, in the new context, the USSR and Romania assured each other of their neutrality (M.F.A.R.–M.F.A.R.F., 2003, doc. 121-122, pp. 249-252); however, on 20 September, V.M. Molotov strongly admonished N. Dianu for Romania's hosting military Polish refugees, considered a danger for the Soviet Union (Ib., doc. 123, pp. 252-253). The previous day, A. Călinescu had noted in his diary that the German danger had receded and the Soviet danger had increased after the collapse of Poland (Călinescu, p. 432).

The rapid succession of events in Poland encouraged Bulgarian diplomacy to advance its own claims. Thus, on 18 September 1939, the Bulgarian diplomat Karastoianov evoked, in Berlin, in front of Ernst Woermann, a scenario that would take shape in the summer of 1940, asking his interlocutor what Bulgaria was supposed to do if the USSR occupied Bessarabia and offered Dobruja (to Bulgaria) *"on a platter"*. The German diplomatic official replied and characterized that scenario as unlikely, at least for the time being, and urged the government in Sofia to maintain a close relationship with Berlin (Sturza, p. 239). On 25 September, Purvan Draganov held a discussion with the USSR's chargé d'affaires to Germany, A.A. Shkvartzev. According to the Soviet version, the Bulgarian minister in the Reich

capital, after expressing his satisfaction with the development of relations between Germany and the USSR, reiterated the Bulgarian arguments concerning Dobruja and Western Thrace, alluding to possible effective Soviet pressure on Romania on the issue of Southern Dobruja and putting British support for Greece on the issue of Western Thrace down to the London government's fears of the possible extension of Soviet influence to the Aegean Sea through a greater Bulgaria (Ib., pp. 242-243). In a telegram sent from Bucharest on 27 September 1939, Pavel G. Kukoliev cited several pieces of information, obtained from the Bulgarian military attaché, according to whom the Romanian authorities had already begun to evacuate archival material from Bessarabia, and that Soviet action in this province was therefore expected (Ib., p. 244).

The Bulgarian diplomacy's insistence on the *"Soviet card"* in September 1939, we believe, must be linked (also) to the categorical signals received from Berlin, in both July and September 1939, to the effect that Germany did not intend to act against Romania, as long as it was satisfied with its economic relations with this country (Ungureanu, pp. 338-344).

An important (diplomatic) episode for the development of the political-diplomatic relations in the Black Sea area, as part of the sequence of dramatic events recorded between 23 August 1939 and 17 September 1939, was the long and not very fruitful visit of Şükrü Saracoğlu to Moscow between 25 September and 17 October 1939. The purpose of the visit was to finalize the Turkish-Soviet bilateral talks, which had begun a few months earlier, by a bilateral treaty of alliance which, in the view of the Ankara government, was to complement the Turkish-British and Turkish-Soviet bilateral declarations (Hitchens, p. 236). After 23 August 1939, however, the relations between the USSR and Great Britain and France were on a downward slope, which could only complicate the Turkish-Soviet talks. Despite this fact and the satisfaction aroused by the conclusion of the Ribbentrop-Molotov Pact, in some Bulgarian circles, fears of a possible Soviet-Turkish pact on the Black Sea persisted in the early autumn of 1939 (Avramovski, 1986, pp. 3335-336). In order not to irritate the USSR, Saracoğlu did not follow Gafencu's suggestion to make a stopover in Romania, either on his way to Moscow or on his return (Collection 71/Türkiye 1920-1944, vol. 61, pp. 217, 222-223); yet on his departure he assured Stoica that he would *"defend Romanian interests as vigorously as Turkish ones"* (Ib., pp. 232, 236).

While the Turkish diplomats (still) hoped to complete the foreign policy work begun in May-June through an agreement with the USSR, the Soviet objectives

in relation to Türkiye, as Saracoğlu's visit to Moscow was to reveal, were quite different. Thus, the Soviet side actually wanted to diminish Türkiye's sovereignty, especially over the Straits, by installing their own military (air-naval) bases in their vicinity, to exclude any military presence of the non-Black Sea littoral states in the Black Sea area, to distance Türkiye from Great Britain and France, but also from its Balkan allies (first of all Romania), which included reconsidering some of the commitments previously undertaken (Hitchens, pp. 236-242; Ekrem, 1993, pp. 98-103; Biagini, 2005, pp. 124-125).

The broader context in which the Turkish-Soviet talks were taking place is also quite important. On 28 September, for the second time in less than 40 days, Ribbentrop arrived in Moscow; on that occasion, the secret bilateral agreements of the previous month regarding the division of Poland and the Baltic area were amended (Constantiniu, pp. 94-98).

At the same time, between 28 September and 10 October 1939, Stalin proceeded to establish a strategic *glacis* in the Baltic area, successively and rapidly imposing on Estonia, Latvia and Lithuania the conclusion of *"mutual aid"* treaties with the Soviet Union and starting negotiations with Finland in order to agree on border *"rectifications"* (Ib., pp. 95-97).

Moscow did not neglect South-Eastern Europe either. To the concern of the decision-makers in Bucharest, at the end of September, the USSR re-established diplomatic relations with Hungary (Haynes, p. 130), which had been severed eight months earlier, and at the beginning of the following month, Bulgaria was the target of a Soviet proposal for a bilateral mutual assistance pact (Miller, 1975, pp. 14-15). The loss of the privileged role that Türkiye had had in the USSR policy on the Black Sea and in south-eastern Europe, in favour of Bulgaria was becoming increasingly obvious; in many diplomatic circles the scenario of a "*Baltization"* of the Bulgarian kingdom, by the installation of Soviet military bases, as in Estonia, Latvia and Lithuania, was being discussed (Avramovski, 1986, p. 336).

According to a Soviet diplomatic document, representing the summary of the discussions held on 1 October 1939, by Saracoğlu with Stalin and Molotov, confronted with an avalanche of demands from his interlocutors, the Turkish Foreign Minister appears to have declared that Türkiye would remain neutral in case of a Soviet-Romanian military conflict over Bessarabia, pointing out, however, that in case of Bulgarian aggression against Romania or Greece, his country would be in a position to react militarily (Sturza, pp. 251-253).

Two days later, Şükrü Saracoğlu met Romania's new minister in Moscow, Gheorghe Davidescu, in the capital of the USSR. In his discussion with the Romanian diplomat, the Turkish Foreign Minister was optimistic about the negotiations with the Soviets, also in relation to the chances of including in the text of the Turkish-Soviet treaty the stipulation that Türkiye's previous commitments to Britain and France did not conflict with the interests of the USSR (M.F.A.R.-M.F.A.R.F., 2003, doc. 132, pp. 265-266).

The Bulgarian Prime Minister, G. Kyosseivanov, was aware of the Soviet pressure on Türkiye, as is clear from a telegram from the Italian plenipotentiary minister in Sofia, Giorgio Talamo, sent to Galeazzo Ciano on 10 October 1939; the head of the government in Sofia and of Bulgarian diplomacy had informed the Italian representative that the USSR was sympathetic to Bulgaria's territorial claims against Greece and Romania (I.I.D., 1993, part two, doc. 46, p. 363).

On 14 October, Davidescu cited information obtained from a French source concerning the Bulgarian minister's activities in Moscow, including his frequent meetings with Soviet and foreign policy leaders, as well as statements in discussions with third parties, to the effect that Germany had left not only the Baltic area to the discretion of the USSR (M.F.A.R.–M.F.A.R.F., 2003, doc. 135, pp. 269-270).

On 17 October 1939 the American Ambassador in Moscow, Laurence A. Steinhardt, after a discussion held *"in the strictest confidence"* with Saracoğlu, dealing with the failure of the Soviet-Turkish negotiations, stated in a report: *"The question of Romania was also raised by the Soviet government in order to obtain assurances of Turkish neutrality not only in case (sic!) the Soviets seize Bessarabia, but also in case the Bulgarians attempt to regain Dobruja"*; the essential cause of the failure of the talks was summarized in a few words: *"Turkish refusal to accept Soviet claims"* (Sturza, pp. 254-255).

On 24 October, Saracoğlu presented to the Romanian Ambassador Stoica the main points of the talks in Moscow. The head of Turkish diplomacy revealed to his interlocutor some of the Soviet demands, namely the obligation for Ankara to consult with Moscow before implementing the obligations assumed under the Balkan Pact, the establishment of a *"German clause"* in the implementation of some of the obligations previously assumed by Türkiye, and undertaking certain obligations in the event of a war opposing the USSR to Great Britain and France. V. Stoica also learned from his interlocutor that he had noted in Moscow a great deal of solicitude for Bulgarian claims. In the same context, Saracoğlu also said that Stalin and Molotov had not explicitly referred to Romania, which was hard to believe.

Asked by the Romanian ambassador what Türkiye's attitude would be regarding the passage of the Franco-British military fleet through the Straits to Romania's aid in case of Soviet aggression, the Turkish foreign minister gave an evasive and vaguely encouraging answer: *"Türkiye will proceed as dictated by its interests in the defence of its territory, determining the concrete course of action in agreement with Great Britain and France"* (Collection 71/Türkiye 1920-1944, vol. 61, pp. 248-252). In March 1940, Şükrü Saracoğlu would admit that he had been asked by Molotov about Türkiye's attitude in the event of an armed Soviet-Romanian conflict, and he had given an ambiguous answer, intended to make the Soviet government cautious towards Romania (Ib., pp. 292-293).

Shortly after the end of the unsuccessful visit of Turkish diplomacy's head to Moscow, the trilateral pact between Great Britain, France and the Republic of Türkiye was concluded (19 October 1939). Under this act, signed in Ankara itself, the three contracting parties were to provide mutual aid in the event of an attack by a European power against Türkiye or in the event of aggression in the Mediterranean. In Article 3, Türkiye undertook to cooperate with Great Britain and France in implementing the guarantees given by these countries to Romania on 13 April 1939. However, in spite of the considerable cooling of Turkish-Soviet relations, the Turkish side requested and obtained the insertion (also) in the text of this agreement of a secret annex, which reiterated the well-known *"Soviet clause"*, i.e. the unwillingness of the government of the Republic of Türkiye to take any action that could have resulted in direct armed conflict with the USSR (I.P.E.R.D., 2003, p. 320).

At any rate, following the signing of this trilateral pact, the favourable character of Türkiye's neutrality (non-belligerency) for Great Britain and France was emphasized, which widened the rift between the Turkish state and its Balkan allies, primarily Yugoslavia. Under those circumstances, one of the basic concerns of Romanian diplomacy was to keep Türkiye within the Balkan Entente, despite the growing Turkish-Yugoslav differences (Avramovski, p. 333). Romania's diplomatic efforts were also facilitated by the way in which the Turkish government understood to relate to the letter and spirit of the treaty of 19 October 1939, constantly avoiding direct involvement in a conflagration and invoking, as a pertinent reason, the insufficient preparation of its military forces (Biagini, p. 126).

The scenario of a possible attempt by the British and French fleets to cross the Straits in order to give aid to Romania on the basis of the guarantees of 13 April 1939, was also a preoccupation of Soviet diplomacy. On 28 October 1939,

the USSR ambassador in Ankara, A. V. Terentiev, raised this issue in a discussion with Ş. Saracoğlu, who initially shied away from a categorical answer, claiming that Romania did not seem to be threatened by any third power at the moment, and then, at the insistence of the Soviet diplomat, assured him that Türkiye would consult with the USSR in such an eventuality (Sturza, pp. 256-257).

At a time when Great Britain and France were at war with Germany, Italy was seen in Bucharest as the only Great Power willing and able to curb the Soviet tendencies of expansion in South-Eastern Europe (Dobrinescu-Pătroiu-Nicolaescu, pp. 243-245). On 20 October, Romanian diplomacy launched its most complete, ambitious and representative project of the *"phony war"* period, namely the *"Neutral Bloc"* initiative. That structure was supposed to bring together as many as seven states, namely the four members of the Balkan Entente, plus Italy, Hungary and Bulgaria. Basically, through this project, Romanian diplomacy aimed at preserving neutrality and normal relations with the three belligerent Great Powers (but also with the USSR), strengthening ties within the Balkan Entente, achieving détente in the relations with Hungary and Bulgaria, but above all, improving (or reinforcing) relations with Italy (I.P.E.R.D., 2003, p. 320).

On the last day of October 1939, a (new) disturbing signal came from Moscow. In his speech (i.e. report) on the development of the international situation and the foreign policy of the USSR, delivered before the Supreme Soviet of the Union, V.M. Molotov spoke, among other things, about the allegedly outdated and inadequate character for the new international situation of the old notions, like *"aggression"* and *"aggressor"* (Dobrinescu, 1991, p. 131). The second leader in the Soviet political hierarchy was thus making a transparent allusion to a number of international acts and documents to which the Soviet Union was (still) a party – first of all, the London Conventions of 3-5 July 1933, on the definition of aggression and aggressor. In the absence of an explicit recognition by the USSR of the unification of Bessarabia with Romania, and in the lack of a bilateral Soviet-Romanian political treaty, these instruments of international law constituted, from Bucharest's perspective, the legal basis for diplomatic relations with Moscow, as G. Gafencu had also pointed out in his broadcast speech at the end of 1938 (Ungureanu, p. 327, note 766).

Türkiye's new position in international relations was also reflected in the traditional annual speech delivered by the President of the Republic, Ismet Inönü, on 1 November 1939, when the new session of the Ankara Parliament opened. Present at that solemn event, Romanian diplomat Gh. Căpităneanu noted that the paragraph in the presidential speech referring to the good relations

with the USSR, which was usually applauded vigorously, that time only elicited weak and complacent applause, in visible contrast to the paragraphs in which the importance of the Anglo-French-Turkish pact was presented and Türkiye's determination to fulfil its commitments was affirmed, which were received with prolonged applause and standing ovations. Căpităneanu also noted the absence of any representative of the German embassy in Ankara and the apathetic attitude of Soviet and Italian ambassadors (Collection 71/Türkiye 1920-1944, vol. 61, p. 253).

EPILOGUE

The Romanian diplomatic initiative of the *"Neutral Bloc"* was to receive favourable but very late responses from Athens (16 December 1939), Ankara (18 December) and Belgrade (21 December), after Romania had abandoned this project for about three weeks (Dobrinescu-Pătroiu-Nicolescu, 1999, p. 249). The failure of the project was primarily linked to the unfavourable attitude of the totalitarian Great Powers, first of all the USSR, followed by Germany, which had initially shown a certain interest, then by Italy, which did not want to assume the role proposed by Romania; in those circumstances, Hungary and Bulgaria, revisionist states, rejected the project, waiting for the right moment to immediately satisfy some of their own territorial claims (Ungureanu, pp 342-345).

The cooling of Soviet-Turkish relations put an end to Romanian hopes of improving relations with the USSR. Through Türkiye, on 4 November 1939, Grigore Gafencu unsuccessfully requested that Germany should initiate the brokering of a Soviet-Romanian non-aggression pact (Haynes, p. 130). Fears of the USSR also prompted Carol II, in the first half of November 1939, to attempt to mediate between Germany and the Franco-British tandem (Ib., p. 126).

Towards the end of 1939, the Romanian-British project to build a military naval base at Tașaul–Năvodari was definitively abandoned (Ungureanu, p. 344), and Great Britain gave an essentially negative answer to the Romanian diplomatic demarches regarding the applicability of the guarantees of 13 April 1939, in case of a Soviet attack on Romania (Lungu–Negreanu, 2000, doc. 33, pp. 209-213).

CONCLUSIONS

In early 1939, the Soviet Union was by far the most powerful state in the Black Sea region, while Türkiye played, or at least appeared to play, the key diplomatic role in the region. In a long-standing friendly relationship with the Soviets and also in a regional alliance with Romania (the Balkan Entente), post-Kemalist Türkiye

was a diplomatic link between Bucharest and Moscow (which was also desired in Romania's capital), and also between Romania and Bulgaria, but without Ankara neglecting its obligations under the Balkan Entente. Türkiye's regional importance was also boosted by its geo-strategic position, especially after it had taken control of the Straits under the Montreux Convention (1936).

Until August 1939, the Soviet initiative for a Black Sea Pact, launched at the beginning of the year, could find support only from Türkiye.

The abandonment by Great Britain and France of their conciliatory policy towards Germany in mid-March 1939 and the diplomatic offensive launched in Central, Eastern and South-Eastern Europe led to or encouraged the emergence of more complex regional projects than the Soviet initiative of February 1939, involving British and French patronage or participation, which lessened some Romanian fears of falling under USSR hegemony. Bulgaria's greatest hopes, however, did not lie in this direction: they were linked to Berlin or a possible or probable German-Soviet rapprochement. Türkiye was firmly committed to cooperation with Britain, France and the USSR, seen as future allies, while Romania was very cautious in that respect, partly motivated by the objective of not provoking Germany, which was to be proved as illusory in the context of the *Reich*'s march towards war.

The conclusion of the German-Soviet agreements in August 1939, the outbreak of the Second World War and the initial course of the hostilities led to a new political-diplomatic configuration in the Black Sea area. Thus, Bulgaria took the place of Türkiye in the regional policy of the USSR, while maintaining privileged economic and diplomatic relations with Germany, and Türkiye continued its rapprochement with Great Britain and France, without renouncing the imperative of not entering into conflict with the USSR.

Of the four countries bordering the Black Sea, it was Romania that felt the shock of the conclusion of the Ribbentrop-Molotov Pact and the outbreak of war the most acutely. Romania's foreign policy objectives during this period were best summarized in the *"Neutral Bloc"* project, launched at the end of October 1939, the failure of which reflected the growing isolation of the Romanian state.

BIBLIOGRAPHY:

1. Arhivele Militare Naţionale Române, Depozitul Central de Arhivă „General Grigore Constandache"/Romanian National Military Archives, "General Grigore Constandache" Central Archive Depository, Pitești, Collection 950 – Ministerul de Război – Cabinetul Ministrului; Collection 5417 – Marele Stat Major – Secţia 2 Informaţii; Collection XIV (studies related to the Romanian Armed Forces).

2. Arhivele Ministerului Afacerilor Externe al României/Romanian Foreign Ministry Archives. Collection 71/Turcia (1920-1944).
3. Avramovski, Ž. (1986). *Balkanska Antanta*, Beograd: Institut za Savremenu Istoriju.
4. Biagini, A. (2005). *Istoria Turciei contemporane*, translated by Ioana Mândrescu. Cluj-Napoca: Editura Accent.
5. Călinescu, A. (1990). *Însemnări politice (1916-1939)*, Al. Gh. Savu (ed.). Bucureşti: Editura Humanitas.
6. Cojocaru, I. (2014). *România şi Turcia actori importanţi în sistemul de relaţii interbelice (1918-1940)*. Târgovişte: Editura Cetatea de Scaun.
7. Constantiniu, L. (2010). *Uniunea Sovietică între obsesia securităţii şi insecurităţii*, Foreword by Acad. Dinu C. Giurescu. Bucureşti: Editura Corint.
8. Dobrinescu, V.Fl., *Bătălia pentru Basarabia*. Iași: Editura Junimea
9. Dobrinescu, V.Fl., Pătroiu, I. (1992). *Ultimele luni de pace: martie-august 1939.* Iaşi: Institutul European.
10. Dobrinescu, V.Fl., Pătroiu, I., Nicolescu Gh. (1999). *Relaţii politico-diplomatice şi militare româno-italiene (1914-1947).* Piteşti-Craiova: Editura Intact.
11. Ekrem, M.A. (1993). *Relaţiile româno-turce între cele două războaie mondiale (1918-1944).* Bucureşti: Editura Ştiinţifică.
12. Gafencu, G. (1992). *Ultimele zile ale Europei. O călătorie diplomatică întreprinsă în anul 1939*, translated by Rodica Mihaela Scafeş, foreword and notes: Cornel I. Scafeş. Bucureşti: Editura Militară.
13. Haynes, R. (2003), *Politica României față de Germania (1936-1940)*, translated by Cristina Aboboaie. Iași: Editura Polirom.
14. Hitchens, M.G. (1983), *Germany, Russia and the Balkans. Prelude to the Nazi-Soviet Non-Aggression Pact*, New York: Columbia University Press.
15. IID (1993) – *Izvori za istoriiata na Dobrudja 1919-1941*, otgovoren redaktor: Petăr Todorov, săstaviteli: Petăr Todorov, Kosjo Penčikov, Marin Ţuţov, Stela Izvorska, Antonina Kuzmanova. Sofiia: Izdatelstvo na Bălgarskata Akademiia na Naukite.
16. I.P.E.R.D. (2003). *Istoria politicii externe româneşti în date*, coord.: I. Calafeteanu. Bucureşti: Editura Enciclopedică.
17. *Istoria românilor* (academic treaties), 2003, vol. VIII, *România întregită (1918-1940)*, coord.: Ioan Scurtu. București: Editura Enciclopedică.
18. Jelavich, B. (2000). *Istoria Balcanilor. Secolul al XX-lea*, translated by Mihai Eugen Avădanei. Iaşi: Editura Institutul European.
19. Kissinger, H. (200). *Diplomaţia*, translated by Mircea Ştefancu and Radu Paraschivescu. Bucureşti: Editura BIC ALL.
20. Kyçyku, K. (2005). *Atatürkismul în Turcia Mileniului Trei*, foreword by Acad. Răzvan Theodorescu, Bucureşti: Editura Adam.
21. Lungu, C.M., Negreanu I.Al. (2000). *România în jocul Marilor Puteri (1939-1940). Documente (1938-1941)*, introductory notes by Dinu C. Giurescu. Bucureşti: Editura Curtea Veche.
22. Mamina I. (1997). *Consilii de coroană*. București: Editura Enciclopedică.
23. Miller, L. M. (1975), *Bulgaria during the Second World War.* Stanford California: Stanford University Press.

24. Ministerul Afacerilor Externe al României, Ministerul Afacerilor Externe al Federaţiei Ruse/Romanian Foreign Ministry, Russian Federation Foreign Ministry (2003). *Relaţiile româno-sovietice. Documente. Vol. II. 1935-1941.* Bucureşti: Editura Fundaţiei Culturale Române.
25. Özden, H. (2013). *The diplomatic maneuvers of Turkey in World War II*, in Karadeniz Araştırmaları Dergisi, Sayi/Year 37, pp. 91-110.
26. Stănciugel, R. (2008). *Lumea balcanică în misiunea şi activitatea diplomatului Vasile Stoica.* Bucureşti: Editura Colias.
27. Sturza, V. (2016). *Basarabia şi destinul ei secret. Mărturii şi documente istorice.* Bucureşti: Editura Litera.
28. Ungureanu G. (2009). *Problema Cadrilaterului în contextul relaţiilor româno-bulgare (1919-1940)*. Brăila: Editura Istros.

NICOLAE TITULESCU AND HIS FOREIGN POLICY IMPLICATIONS FOR THE BLACK SEA SECURITY

Daniela Florentina BORCAN
Romanian National Military Archives
DOI: 10.55535/RMT.2024.4.50

Romania has promoted an active foreign policy that aims to defend independence, territorial integrity, and develop security to ensure peace. Nicolae Titulescu, who was the main figure in Romanian foreign policy, safeguarded the country's borders during challenging times, taking into account the importance and advantages of our territory. The political man focused on the Black Sea and the issue of the straits. In a conciliatory framework, Titulescu supported strategic cooperation and advocated the conclusion of regional alliances and conventions to harmonize the interests of peoples, resulting in strengthening security in the face of expansionist trends as well as in enhancing trade and free movement of vessels in the Black Sea.

Keywords: Nicolae Titulescu; military power; Black Sea security; strategic cooperation; Montreux Convention;

Motto: "I would say that the Straits are the heart of Türkiye, but they are at the same time the lungs of Romania. When a region, through its geographical situation, is the heart of a nation and the lungs of another, the most basic wisdom dictates that these two nations should unite and make one whole".

Nicolae Titulescu

INTRODUCTION

Security in the Wider Black Sea Area is the subject of interest of Romanian historiography, the research involving a complex analysis that covers several aspects, not only geopolitical and strategic, but also historical ones. The present paper has as its main research objective the importance of the political events in Romania's interwar period, especially the importance of foreign diplomacy carried out by the politician Nicolae Titulescu and his key actions regarding Romania's contribution to the security of the Black Sea.

Nicolae Titulescu, one of Romania's most prominent diplomatic figures in the interwar period, was well known for his role in international politics and had a significant impact on the evolution of Romania's foreign policy. Through his intense diplomatic activity and international cooperation, he promoted the principles of collective security in the Wider Black Sea region, an area of strategic interest for several powers, including the Soviet Union, Türkiye and littoral states such as Romania and Bulgaria.

The regime was marked by territorial tensions, as well as competition for influence in the Balkans and the Caucasus. Romania, having an extended border along the Black Sea and controlling the mouths of the Danube, had vital security interests linked to this region, including maintaining stability and a favourable balance of power.

FOREIGN POLICY DIRECTIONS FOR ACTION

Regarding Nicolae Titulescu's foreign policy, he pursued multiple directions of action concerning the principles of security, as both a supporter and a promoter of those principles. In addition to the regional alliances Romania joined, aimed at ensuring its security, such as the Little Entente (an alliance between Romania, Czechoslovakia and Yugoslavia), he also supported collective security. The concept

of collective security in the European system, advocated by Titulescu, promoted cooperation between European states to prevent wars and ensure stability. Those alliances were aimed at maintaining the balance of power in Eastern and Southeastern Europe as well as at protecting Romania from potential aggression, including in the Black Sea region.

Titulescu supported stability in the Black Sea region and was actively involved in various negotiations and discussions aimed at preventing the expansion of foreign influence in the area. By attempting to build good neighbourly relations, he advocated for peace treaties that would ensure stability, such as the Treaty of Lausanne in 1923. The treaty redefined borders and power relations in the Balkans and the Black Sea region after the First World War. Although Titulescu was not directly responsible for drafting the treaty, he was involved in its ratification, working to achieve a favourable balance of power in Romania. The international agreement established the borders of the Republic of Türkiye, reorganizing the balance of maritime power. A principal and important provision of the treaty was the recognition of Türkiye's sovereignty over the Bosphorus and the Dardanelles Straits, granting Türkiye the right to exercise control over them.

The balance of power mentioned earlier concerned Romania's geopolitical position, particularly from the perspective of the international regime of the straits, the freedom of navigation in this area, and Romania's access to the Black Sea. The Treaty of Lausanne laid the foundation for regional cooperation in the Wider Black Sea Area and for the collaboration between Türkiye and its neighbours. Romania benefited from the regional stability essential to this treaty, especially since one of its advantages was free maritime trade.

Being aware of the importance of maintaining peace and balance in the area, Titulescu became one of the architects of the Balkan Pact in 1934, signed between Romania, Greece, Yugoslavia and Türkiye, with the aim of consolidating resistance against revisionist aggression, including in the Black Sea region. The Balkan Pact guaranteed the consolidation of Romania's borders, established after the First World War, and the strengthening of relations with Türkiye, aiming to ensure the stability of the region. The Balkan Pact materialized Titulescu's vision of a stable Europe that would prevent armed conflicts.

Closely related to the aforementioned treaties is the Montreux Convention, signed in 1936, after the Conference on the Regime of the Black Sea Straits, which was held with the aim of establishing a new regime on the straits. The convention regulated the regime of the Bosphorus and the Dardanelles Straits, which made Titulescu directly interested in the consequences of the Convention. Thus, Titulescu

was trying to support the idea that Türkiye should regain power and control over these straits, fearing that, otherwise, destabilization would occur in the region.

The new convention replaced the Treaty of Lausanne in 1923, which had established international control over the straits. Titulescu supported the new situation because the arrangement was much more favourable to Romania from the point of view of security in the Black Sea region. The reasons why he supported the Convention were pertinent and concerned the future of Romania's security, diplomatic relations, the right to free passage of ships, the issue of trade, the future of the economy and the geopolitical context. In addition to reducing the risk of invasion by the revisionist powers, the convention guaranteed the situation of commercial ships, their free passage during peacetime, which was essential for Romania's international trade.

At the same time, in the event of a war situation, Türkiye had the right to restrict the access of foreign ships to the Black Sea region in order to protect the maritime space from external invasions. An important role was also played by the International Straits Commission, with representatives such as those of Türkiye, Greece, Romania, Bulgaria and Russia, who had in mind the observance of the regime of the straits, an objective continued by the partner countries under the provisions of the Montreux Convention. For Romania, the situation of the straits was one of particular importance, taking into account the effects of navigation on the Danube. Movement on the river led the economic development of Romania.

In the 1930s, the European space faced the rise of new totalitarian political ideologies, which endangered its political and territorial integrity. For European peace, the expansion of fascism and nazism was a real danger that the nations had realized quite quickly. Nicolae Titulescu also played an important role in the normalization of Romania's relations with the Soviet Union in the 1930s. Although cautious, he considered it essential to maintain a diplomatic dialogue with Moscow in order to protect Romania's territorial integrity, especially in the context of the disputes related to Bessarabia and the Black Sea security.

The relations with the USSR were based on collaboration and prudence, on dialogue and bilateral cooperation, arguing that an understanding with the URSS could offer Romania more security, a counterbalance trying to introduce Russia into collective security alliances. As expected, Titulescu was criticized for his policy of cooperation with the USSR, especially by the conservative side that feared the great power changing attitude. Here we recall Gheorghe I. Brătianu, who expressed his mistrust and concern towards Titulescu's actions, which he considered especially dangerous, as the future and defence of Romania could

fall into the hands of Moscow. Undoubtedly, his policy had both positive effects, maintaining some tranquillity and peace regarding Romania's position in the face of regional tensions and less favourable effects with the dismissal of Titulescu. The tensions regarding the future of Bessarabia, a subject that remained sensitive even after the diplomatic discussions held between Romania and the USSR, prevented a permanent collaboration, creating a much more tense and difficult to manage framework for Romania, culminating in the Soviet ultimatum of 1940.

Through his efforts to build a collective security system and through the regional alliances he supported, Titulescu indirectly contributed to the stability of the Black Sea region. It was crucial for Romania, which depended on a stable regional environment to protect its economic and strategic interests in the area. Titulescu used the international tribune of the League of Nations to promote disarmament and the peaceful settlement of disputes, including in the regions adjacent to the Black Sea. Although his success was eclipsed by the rise of totalitarian regimes and the failure of the League of Nations, he set a precedent for Romania's subsequent approaches.

CONCLUSIONS

Titulescu's diplomatic legacy influenced Romania's foreign policy even after his death, including in the post-war period. The principles of collective security and dialogue that he promoted continued to be relevant in the policy towards the Black Sea, especially within NATO and other international organizations. In the current context of tensions in the Black Sea region, Titulescu's ideas on active diplomacy, international cooperation and conflict prevention remain important for Romania's approach to managing security challenges in the area.

In conclusion, his diplomatic activity had a significant impact on collective security. He contributed to the creation of a diplomatic framework that influenced the stability and the security of the Black Sea, a crucial aspect for Romania's foreign policy in the interwar period. As the head of Romania's diplomacy, he campaigned for peace, security, the people's right to independence and unity. The preservation of territorial integrity was also an objective of Titulescu's foreign policy. However, he was criticized in the contemporary period for the actions of approaching the USSR, being categorized as dangerous and even strange. Throughout his career, the great diplomat launched original, peaceful, courageous ideas, especially within the League of Nations, in a dangerous context, under the expansion of totalitarian regimes. His actions, carried out more than 80 years ago, still have effects today, which proves once again the power and dedication of the great politician.

BIBLIOGRAPHICAL REFERENCES:

1. Arhivele Militare Naționale Române/Romanian National Military Archives, Fond Microfilme 948/Microfilm 948 Collection, *Secția 3 Operații/Section 3 Operations*.
2. Bărbulescu, P., Cloșcă, I. (2022). *"Repere de cronologie internațională 1914-1945".* București: Editura Științifică și Enciclopedică.
3. Botoran, Const., Zaharia, Gh. (1981). *Politica de apărare națională a României în contextul european interbelic (1919-1939).* București: Editura Militară.
4. Calafeteanu, I. (1997). *"Politică și interes național în România interbelică"*. București: Editura Enciclopedică.
5. Ciachir, N. (1996). *"Marile puteri și România (1856-1947"*. București: Editura Albatros.
6. Oșca, Al. (2003). *"Managementul crizelor regionale. Modelul balcanic interbelic".* București: Editura Academiei de Înalte Studii Militare.
7. Oșca, Al., Nicolescu, Gh. (1994). *"Tratate, convenții militare și protocoale secrete (1934-1939)".* Pitești: Editura Vlasie.
8. Retegan, M. (1997). *"În balanța forțelor. Alianțe militare românești interbelice".* București: Editura Semne.
9. Talpeș, I. (1988). *"Diplomație și apărare.Coordonate ale politicii externe românești (1933-1939")*. București: Editura Științifică și Enciclopedică.
10. Titulescu, N. 1937 *"Relațiile dintre România și alte state",* in *"Politica externă a României* (1937)".

MILITARY ACTION IN SECURING AND RESTORING ORDER DURING THE POGROMS IN BESSARABIA IN 1903 AND 1905

Artur LEȘCU, PhD
State University of Moldova, Chișinău, Republic of Moldova
DOI: 10.55535/RMT.2024.4.51

The Russian Empire, an autocratic state with strong remnants of feudal caste law, was based on a legal system that aimed to intimidate the citizenry in order to defend and preserve the existing anachronistic social order. Various specialized state institutions were responsible for the security of the regime and internal order, among which the armed forces. The tsarist authorities widely used military units in the fight against mass demonstrations and the preservation of public order. In this paper, based on the vast new documentary material from the national archives of the Republic of Moldova, we will demonstrate the actions of the military units in order to save the Jewish population of Bessarabia during the pogroms of 1905 and 1907.

Keywords: Bessarabia; pogrom; regiment; infantry; self-defence;

INTRODUCTION

At the beginning of the 20th century, the Russian Empire had a vast Jewish diaspora, deprived of political and civic rights following the adoption of a whole series of anti-Jewish laws, required to reside in pre-established exclusive areas of residence. According to the first general census of the Russian Empire, held at the end of the 19th century, 5,215,825 Jews lived in the empire, which constituted 4.15% of the entire population, of which in Bessarabia – 229,000, that is 11.7 % of the population of the region (Nistor, 1991, p. 213). The massive concentration of the Jewish population in the urban centres of Bessarabia led to numerous anti-Semitic tensions, which sometimes ended with the outbreak of violence in the form of pogroms, the most famous of which is the pogrom in Chișinău, from 1903.

THE POGROM IN THE SPRING OF 1903 IN CHIȘINĂU AND THE ATTEMPTS OF THE ARMED FORCES TO REPRESS THE MASSACRES

Since March 1903, the Gubernial Directorate of the Independent Corps of Gendarmes in Bessarabia, through its head, Colonel V. Charnoluskij, and his subaltern, the rittmaster, Baron von Levendal, head of the guard section of Bessarabia Department for the Defence of Public Security and Order (Ohranka), warned the authorities of St. Petersburg about the tense situation created in Chișinău and the imminent outbreak of a massacre on the Jewish population in the city (Новицкий, 1991, p. 177). Due to them, the gubernial authorities, in the person of the governor, Lieutenant General Rudolf von Raaben, sensing that, on Easter eve, the spirits were getting hot in the city, strengthened the city guard, detaching armed patrols from the military garrison of Chișinău to the police. At that time, the Chișinău garrison was an imposing military force, composed of two infantry regiments (53rd Volania Infantry Regiment and 54th Minsk Infantry Regiment), a reserve infantry battalion (207th Chișinău Reserve Infantry Battalion), an artillery brigade (14th Artillery Brigade) and a cavalry regiment (24th Lubensk Dragon Regiment). However, what followed also surpassed the bleakest predictions about the existing situation. For three days, between 6 and 8 April 1903, the city was engulfed in the explosion of a deadly hatred towards the Jewish population, degenerated into the massacre.

51 people were killed, 456 were injured, 1,350 homes of the 4,149 existing in the city were vandalized (Джадж, 1998, p. 86), the amount of damage amounting to about two million rubles (Ib.). In such cases, the main question is how could such a thing happen, who was the culprit, and where were the armed forces?

We must examine this question in the context of previous investigations, paying special attention to the analysis of overlooked moments in the past that can shed new light on the course of events. Most researchers observed that the events were unexpected by local authorities, who were not expecting a crisis. As in previous years, the patrols deployed to the police bodies from the military units were not numerous, the reserve being composed of several groups gathered from all the infantry units of the garrison, without internal cohesion and single command, the number not exceeding 1.5 infantry companies (Кишиневскийпогром, 2000, p. 224). The military authorities allowed soldiers to freely exit the city, on 5 April, to participate in the midnight Easter service. Despite the increasingly tense situation in the city, the permissions were not cancelled for 6 April. However, the commanders told the military to return to the unit in the event of an exceptional occurrence. The commanders' decision made it hard to gather the units on alarm and use them efficiently when necessary. In the case of the 54th Minsk Infantry Regiment, which was gathered in its full composition on 6 April, well after 16:00, some of the soldiers returned from leave were intoxicated (ASPORM, collection 90, inventory 3, file 5, p. 2). Not all the soldiers on leave arrived at the units, some of them, unidentified, were observed among pogromists, such as the soldier Ion Burduja, who was on leave, as well as former servicemen, demobilized from the army, Ion Vacari, Pavel Veto, Vasile Sarban, Anton Dulghier, Fyodor Gornostaev, Macarie Malasenco (Кишиневскийпогром, p. 278). The occasional participation of the military (former and active duty) in the events, with their combat experience, explains why the pogromists were acting methodically, based on *"a plan"* (Джадж, p. 64), but spontaneously, which excludes the hypothesis that the massacre was organized and directed by obscure forces, not yet elucidated.

The first day of the massacre, 6 April, demonstrated that police bodies, reinforced with military patrols, were barely coping with the events in their early stages. The police justifications for the lack of staff (213 policemen for a city with a population of over 100,000 inhabitants) are out of criticism and would be correct under conditions of lack of an army aid. Joint patrols, which consisted of soldiers and policemen without any orders to fire, were under the general command of police workers, but were utilized inefficiently due to the lack of communication and coordination of actions between them. The chief of police, A. Hanjenkov, though former career military and senior officer in the cavalry, instead of taking over the general

command over the operation of repressing the pogrom, during the period between 13.00 and 16.00, was traveling on the streets of Chișinău, inspecting the main markets where people gathered agitated, urging them to scatter, action that was at hand of a sector policeman and the police chief. The scattering of the aggressive crowd on the Ciuflea market, which took place after 16.00, was not followed by the operation of mass arrests of aggressive people. Even those arrested were released from the hands of the police by their comrades, indicating the impossibility of the police and the army to respond to the crowd (Кишиневскийпогром, p. 218). The dispersed crowd, yet not arrested, spread through the streets adjacent to all the districts of the city, clustered around informal, aggressive leaders, some with military experience, forming small bands in the number of 10-20 people, having children in the vanguard, strengthened by adults in the second echelon. Soon, simultaneous unrest began in several parts of the city. Joint patrols of the military and police were forced to act separately from each other, on several directions, in the absence of coordination and the linkage system established in advance, dispersing the common effort of the law enforcement forces, few in number and without a consistent reserve. It was not due to the existence of a plan drawn up in advance by anonymous leaders of the massacre, but to the logic of the events and mistakes admitted by the authorities, of which the pogromists took full advantage. Among the errors committed by the authorities was that the cavalry was not involved in scattering the crowd divided into small groups, the cavalry being the only military force capable of acting at high speed in the city streets. Only in the evening, after he realized that he could not keep the situation under control, the police chief, A. Hanjenkov addressed the governor of Bessarabia, Lieutenant General R. von Raaben, who in turn redirected him to the head of the Chișinău garrison, Lieutenant General V. Bekman, where A. Hanjenkov arrived only after 20:00 (Ib., p. 224), when the situation in the city had already calmed down. Following the consultations, it was decided that, on 7 April, 9 infantry companies and 6 cavalry squadrons would be deployed to police bodies, without the right to open fire (Ib., p. 225). It caused further violence, starting on the morning of 7 April. And that time too, the military and the police did not act in coordination, passing responsibility from one to the other. Considerable military forces were concentrated in the central park, waiting for an alleged political demonstration that did not take place. However, because of that expectation, they were stationed until noon, instead of participating in the suppression of disorder. Considerable military forces were deployed to guard the homes of the infantry brigade commander, Major General Glebov, and the commanders of regiments and battalions, as well, being excluded from actions of restoring the rule of law (ASPORM, collection 90, inventory

3, file 5, p. 3). The passivity of the mixed military-police teams, who understood their task in guarding the communication arteries and dispersing the crowd, not wanting to sanction the arrests (Кишиневскийпогром, p. 333), unleashed the crowd, the Jews being simultaneously assaulted in all the districts and suburbs of the city. More determined in the scattering of the aggressive crowd were the dragons, but also in their case the criminal ingenuity of the killers found its way out in a tactical combat process – sneaking, one by one, among the cavalrymen's horses (Ib., p. 260). The authorities failed to control the situation in Chișinău.

At 15:30, taking into account the gravity of the situation, the governor of Bessarabia, R. von Raaben, delegated, in writing, to the head of the military garrison in Chișinău, Lieutenant-General V. Bekman, all powers in the suppression of massacres, with the right to open fire. At 16:00, General V. Bekman issued an order on the garrison to assume full power, dividing the city into several sectors, distributed to units with the right to use the weapons. Starting at 17.00, after the order was brought to the attention of the staff, measures started to repress the pogrom, making mass arrests, which were carried out quite quietly, and, it was not necessary to open the fire, using only the bayonets and the weapon grips in the inventory. The authorities were able to control the situation by midnight, except for the suburbs where the massacres continued until 8 April in the evening. In the massacres and killings in the suburbs were involved the Moldovan population, thus excluding the influence of the written press, even the newspaper of P. Crucevan, because that population, in its majority, was illiterate.

In conclusion, we can say that the pogrom in April 1903 in Chișinău was based on the frustrations and grudges of a part of the pauperized population of the city, accumulated over several years against the Jewish community, spurred by verbal rumours, the role of the press, including reactionary, being marginal in a predominantly illiterate region. The magnitude of the tragedy was due to the confusion of the leadership of the governorate, who, at the moment, failed to exercise its power. The actions of the authorities were characterized by the lack of a single leadership, coordination of crowd repression actions, fear of opening fire on demonstrators and conducting mass arrests among the rebels. It was only after the authorities returned from the shock, losing a day and a half, that they began to act concentrated and efficiently, using military force to extinguish the outbreaks of massacres existing in the city.

MILITARY ACTIONS IN THE SUPPRESSION OF JEWISH MASSACRES IN 1905

More serious consequences and amplitude had the pogroms in Bessarabia in October 1905, which is less known, being practically ignored in historiography. On 17 October 1905, after the news about the issuance of the Proclamation by Nicolai II on improving the state order, the revolutionary forces participated in a political rally, where about 10,000 people gathered. In opposition to that rally, the pro-government forces planned a patriotic demonstration in support of the monarchy and the rule of law on 18 October. On the morning of that day, about 5,000 people gathered in the Ciuflea square, from where they started, at 11:00, to the Cathedral, holding the Russian national flags and portraits of Nicolai II. At the intersection of Armenian streets with Aleksandrovskaya (Bld. Stephen the Great), on the demonstrators, a fire salvo was fired by some unknown people, which caused the aggressive reaction of the crowd. The vicinity of the New Square (now Central Square) determined the crowd to begin looting, temporarily stopped by the rittmaster of the independent body of the Vasiliev gendarmes, delegated by the authorities to accompany the demonstration. The situation repeated itself at the next intersection with str. Kupeceskaia (current str. Vasily Alecsandri). Again, the situation was saved by the Vasiliev commissioner (NARM, collection 297, inventory 1, file 40, p. 1 verso). Arriving in the cathedral square, the demonstrators took part in the prayer, when, unexpectedly, the bellboy on the cathedral bell tower began to shout that the Jews were robbing the shops of Gottlieb Gheer and Raymond Ghikish, where, among other things, firearms were sold. It is unclear how the boy, from a height of 40 meters, observed the nationality of looters operating on two neighbouring directions, even if at short distances from each other. The hectic crowd triggered the pogrom, which spread to all the districts of the city. Taking into account the experience of the 1903 pogrom, Bessarabian governor Alexei Haruzin convened an emergency operative meeting to which the commanders of the military units from the garrison were invited. At that meeting, it was decided to establish special police detachments for tracking pogromists, military units were given the right to open fire, including artillery, against the rebel resistance centres. In order to isolate the city from the suburbs and agrarian areas, detachments of free peasants were set up to stop other peasants on the way to Chișinău. Towards the end of the day, under threat of firearms, the massacres were stopped, but they resumed on 20 October, when rebel groups opened fire on the soldiers, killing and pillaging Jewish houses and shops. The use of armed forces, including several cannon salves, ended the massacre. Between 18-20 October, 55 people were killed and 107 injured

(Ib., p. 2), 89 houses and shops were vandalized and looted, among them being those that did not belong to the Jews, such as that of Princess Evfrosinia Viazemskaiasau of Tudor Grițan, the amount of damage constituting about 24,690 rubles (Ib., pp. 2-11).

Unlike in 1903, the pogroms of 1905 spread throughout Bessarabia. The beginning was on 22 October, when the pogrom against the Jewish population in the locality broke out in Strășeni. Due to its proximity to the gubernia capital, the massacre was repressed on the same day (Ib., p. 17). Much worse was the situation at Akkerman (White Citadel), where, on 18 October, a political demonstration was held, turning into a general strike. Russian nationalist circles in the city obtained permission from the city hall to hold the rally in support of the government and the monarchy on 22 October. The head of the police, contrary to the rally, refused to provide police assistance in supervising the event, leaving the demonstrators to fend for themselves. After the divine service at the Cathedral, the demonstrators, with national flags, portraits of Nicolai II, intoning the national anthem, marched through the streets of the city and set off for the fairs Popusoi (Peremozhnevo) and Turlaca (Vypasne), the suburbs of Akkerman. There, they were joined by a group of locals, armed with bats, crowbars, axes and revolvers, who, along with the rest of the crowd, began to burn and rob Jewish houses and shops (Ib., p. 50). Upon returning to the city, the agitated crowd was stopped by a company of soldiers, but, bypassing it on the side streets, they entered the locality, thus starting the pogrom. Despite the fact that the army began to shoot at the aggressors, between 18:00 and 04:00, all Jewish shops were burned and destroyed, the city being engulfed in flames. Only after an additional company of soldiers was sent to Akkerman (White Citadel) in Bender (Tighina), the situation in the city was taken under control.

On 23 October, the bloodthirsty inhabitants of Popusoi (Peremozhnevo) and Turlaca (Vypasne) tried to enter the city again, but they were stopped by the fire of the army. As the Vasiliev rittmaster, chief aid to the Governorate of the Independent Corps of Gendarmes, mentioned in his report, the Russians in Popusoi (Peremozhnevo) and Turlaca (Vypasne) turned into real bandits, gathered in groups of 6-10 people armed with revolvers, who did not recognize any authority, terrorizing the wealthy sections of the population, including Russians, extorting from them money and material goods (Ib., p. 5). The Russian population at the Shabo (Shabo) fair, urged by the exploits of its fellow countrymen in Popusoi (Peremozhnevo) and Turlaca (Vypasne), attempted to plunder the local Jews, but they were stopped by armed patrols of French and German settlers, who, opening

fire, killed 2 and wounded 3 attackers. On 25-26 October, incidents occurred in the localities Divizia, Chebabcea (Shyroke), Monași (Monashi), Bairamcea (Mykolaivka), resulting in looting the Jewish population in these localities. It was hard and with the help of the army to restore order in the land of Akkerman (White Citadel). 70 people, Russian and Jewish, were killed and wounded (Ib., p. 50 verso).

A serious situation was also in Ismail, where, on 22 October, between 19:00 and 21:00, a political rally was organized in the city centre by revolutionary circles, at which were discussed the political consequences of the Proclamation of 17 October 1905. After the rally, some of the participants, representing the unskilled workers in the port, some of them under the influence of alcohol, moved to the shopping district, where they began to destroy the Jewish little shops (Ib., p. 34 verso). The situation in the city worsened dramatically on 23 October, when, starting at 12:00, the crowd, numbering about 200 people, composed of teenagers and workers, started to burn and destroy the Jewish shops. The city authorities, in a state of confusion, repeated the mistakes made by those in Chișinău, in 1903, being unable to resist the massacres, in conditions where they had local police reinforced with two platoons of the Independent Border Corps. It is also worth mentioning the behaviour of the collaborators of the gendarmerie corps who, in the tragic events of Ismail, made efforts to appease the spirits. Thus, sergeant Moisei Seledin and vahtmaster Semion Savel put out the fire that engulfed a shop, and sergeant Anton Carlashevschi defended on the streets of the city a large Jewish family from the rage of the crowd, saving them from death. In contrast, it was the behaviour of the local clergy, who involuntarily, instead of settling, stirred the spirits. Arriving in the evening of 23 October at the *"New"* Square, which was covered with flames, the clergy, wearing festive garment, with crosses and flags, was greeted by the crowd with cheers and shouts *"Hooray"*!. Stopping from the robbery during the clergy's urges to stop the massacre, the crowd immediately continued its criminal activity after the religious procession moved to the next burning object. Under the conditions when all the commercial part of Ismail was caught in flames, several hundred Jews, with the permission of the head of the customs, took refuge on a barge from the port of Ismail, in the customs department of Ismail, from which the walkway was removed to prohibit access at night (Ib., p. 35 verso).

To put an end to the pogrom that continued through the night, Colonel N. Rogovschi, the commander of the Ismail Border Brigade, strengthened the local troops with guard troops, moving to action, starting at 01:00, with the rest of the troops in the city, opening fire on the attackers. Towards 05:00, on 24 October, following the energetic actions of the soldiers, who, at night, by the opening

of the fire, killed 10 people and wounded 11, all unskilled workers, order in the city was restored (Ib., p. 37). However, the city was still panicked and many Jewish families and state officials crossed the Danube and took refuge in the Romanian villages of Satul Nou and Tulcea. With the introduction, on the streets of the city, of pedestrian and horseback patrols, the situation was taken under control, the city, starting on 25 October, returning to normal life. After the south, the centre of Bessarabia exploded. It all started in Călărași, on 23 October, the day of the fair, when many people from neighbouring villages gathered to do shopping. Around 10:00, a gunshot was heard that sparked the rage of the crowd, mostly composed of Moldovans, who began the devastation of shops and homes of the Jews. The town centre was set on fire, burning up to 150 Jewish houses. The Jewish population, about 2,000 souls, took refuge in the building of the state's former wine warehouse. Upon receiving the news about the outbreak of the pogrom in Călărași, there, by rail, was sent deputy governor S. Tatishchev, accompanied by a company of soldiers. When S. Tatishchev arrived at the scene, he blocked the village entrance for peasants in nearby villages and re-established order by opening fire against the robbers. In general, 40 people were killed following the pogrom in Călărași, most of them Jews, 5 of whom were burned alive (Ib., p. 26).

On 23-25 October, pogroms took place in the towns of northern Bessarabia – Mîndra, Dereneu, Rădeni, Hirova, Hoginești, Onișcani, Pitușca, Hîrtopul Mare, Paustova, Bîrnova, Bahmut, in which at least 14 Jewish households and dwellings were destroyed and 4 people were beaten, including peasant Peter Mezdra, cruelly beaten by the attackers, because he defended the Jewish families (Ib., pp. 47-48 verso).

CONCLUSION

Jewish pogroms in the autumn of 1905 had a much larger character than those in 1903, in Chișinău, 105 victims (killed) were certainly attested, and 70 people killed and wounded, without exact distinction, a total of 175 people (Ib.). The area of massacres encompassed the entire region, both urban and agrarian settlements. The practically simultaneous actions of the revolted in different geographical parts of Bessarabia suggest the existence of an alleged coordinating centre planning the deployment of pogroms. However, the documents in the archive do not confirm the existence of such a centre, which does not allow us to draw that conclusion. The 1905 pogrom, unlike the 1903 pogrom, had no media influence on the outbreak of massacres, which confirms the minor role of the press in the events of 1903.

At that time, the authorities reacted promptly to the challenges that arose, making extensive use of the armed forces, which acted in an organized, prompt and energetic manner, unhesitatingly opening fire on the robbers and murderers, hence the large number of victims. The lesson given by the authorities to the anti-Semitic elements was assimilated in the region as, until 1917, there were no anti-Jewish pogroms documented.

BIBLIOGRAPHY:

1. Arhiva Națională a Republicii Moldova/ National Archive of the Republic of Moldova/ ANRM, collection 297, inventory 1, file 40.
2. Arhiva Organizațiilor Social-politice a Republicii Moldova/Archive of Social-Political Organizations of the Republic of Moldova/AOSPRM, collection 90, inventory 3, file 5, p. 2.
3. Новицкий, В. (1991) *Из воспоминаний жандарма*. Москва: Издательство МГУ.
4. Nistor, I. (1991) *Istoria Basarabiei*. Chișinău: Cartea moldovenească.
5. Джадж, Э. (1998) *Пасха в Кишиневе. Анатомия погрома*. Кишинев: Лига.
6. Кишиневский погром 1903 года. (2000). *Сборник документов и материалов*. Кишинев: Ruxanda.

LESSONS LEARNED BY THE ROMANIAN ARMED FORCES AFTER THE 1916 MILITARY CAMPAIGN

Lieutenant Colonel Ovidiu PĂDURARIU
"General Gheorghe Mărdărescu" Regional Military Centre, Iași
DOI: 10.55535/RMT.2024.4.52

The military actions of the Romanian Armed Forces in 1916 gave rise to valuable lessons learned, some still applicable today. Of course, the proportions regarding the evolution of weapon systems, the diversification of military specialties, the emergence of hybrid actions, the accession to international alliances must be preserved. Nevertheless, the actions remained the same. On today's battlefield there is various equipment, technological and intelligent, that existed in rudimentary forms even 100 years ago. Although the equipment has evolved and diversified unimaginably, the goals and actions have essentially remained the same. A good example is the recent conflict in Ukraine, where, although we are talking about intelligent systems of detection, selection and hitting of targets, everything has been reduced to a ground confrontation, conquest of territories, employment of forces in the open field and localities, use of different techniques, tactics and actions like those of the First World War. Therefore, the analysis of past battles, such as the campaign of 1916, is not a pointless activity, but an exercise in analysis and thought, whereby old, not obsolete, tactics are superimposed on current conflicts.

Keywords: First World War; Romanian Armed Forces; military campaign; goals; lessons learned;

INTRODUCTION

The result of the military campaign in 1916 had disastrous effects to Romania: the territory and population, under occupation, were exploited to the maximum by the Central Powers, Dobrogea was conquered by Bulgaria, the Carpathian passes were controlled by the Austro-Hungarian Empire, a considerable amount of military equipment had been lost, the national infrastructure suffered major destruction, and the morale of the troops dropped considerably. However, our country resisted the offensive of the Central Powers, withdrawing to Moldova in order to restore and reorganize the armed forces, for the resumption of military actions. Among the reasons that prevented the total defeat of Romania can be listed the exhaustion of the enemy, the precarious condition of the roads, as well as the military aid of the Russian Empire to stabilize the front in Moldova. In the situation of the outbreak of the Russian revolution a year earlier, most likely the situation of our country would have been critical, the front in the Moldavian area becoming much weaker and more *accessible* to the enemy.

There were many opponents in relation to the moment chosen for our country's entry into the war, who cited some favourable situations for the Entente, when it was in advantage on the European fronts. Prime Minister Ion I.C. Brătianu was accused of over-negotiating the terms of entry into the war, while the Central Powers were under pressure at Verdun, the Isonzo and in Galicia. However, the Romanian Government sought to put in place all the details for entering the war: well-equipped and prepared armed forces, support actions from the Allies, as well as guaranteeing the fulfilment of the national ideal of unifying the Romanian territories, in the subsequent peace negotiations.

An often-cited reason for the military failure in 1916 was the insufficient equipment of the Romanian troops. During the two years of neutrality, measures were taken to adequately equip the armed forces, especially in terms of providing them with armaments, ammunition and other equipment. It was possible both by allocating significant amounts of money and by improving domestic production. Therefore, if upon entering the war, the Romanian armed forces were considered insufficiently prepared, most likely, 1-2 years before, it would have been at an even lower level.

The term *lesson learned* is used in a broad sense to describe people, things and activities with the aim of learning from experiences and gaining advantages for the future. Using lessons learned helps individuals and/or the organization reduce the risk of facing the same problems and increases the chances for success (The NATO Lessons Learned Handbook, 2022, p. 9). The goal is to effectively learn from past experiences and provide validated justifications for performance improvement. Specifically, lessons learned are absorbed and practiced in the training process so that troops are properly prepared for the current, changing challenges of the battlefield [Joint Publication (AJP)-3(C)2019, p. 149]. In order to issue lessons learned, conclusions or teachings, answers to the following questions should be provided:

- *What was supposed to happen?*
- *What actually happened?*
- *What was well and why?*
- *What did not go well and why?*
- *What lessons and conclusions can be drawn?*

The papers that analyse the military campaign of the Romanian armed forces in 1916 are varied and influenced by the authors, especially those directly participating in the conflict. Among them are distinguished those who were on the battlefield and those who planned military operations within the General Staff Headquarters. Although they represent valuable sources, they are marked by a very high degree of subjectivity, given personal affinities. Memoirs are subjective works that present the facts through the author's perspective, based on personal experiences at the time. In addition, the military leaders, through their own writings, apologize, look for culprits or, on the contrary, amplify their own decisions and actions, depending on the result obtained. Many papers have inserted, in their content or in specially intended chapters, a series of important conclusions for the subject under analysis.

MILITARY OPERATIONS OF THE ROMANIAN ARMED FORCES FROM AUGUST TO DECEMBER 1916

Between 1914-1916, Romania remained neutral, carrying out negotiations with both the Entente and the Triple Alliance, for entering the war. On 4/15 August 1916, our country allied with the Triple Entente, political-military bloc, and undertook to start military actions until 17/28 August.

Following the analyses of the options for action, taking into account the aspirations of the Romanian people for the achievement of the unitary state, the General Staff adopted Hypothesis Z, which provided for an offensive operation

in Transylvania and a defensive one on the front with Bulgaria. The campaign plan, officially called the *Plan of Operation for a War against the Central Powers and Bulgaria. Romania allied with the Quadruple Entente* (Toma, Boaru, 2018, p. 74), also defined the political objective of the war: *"the achievement of our national ideal, i.e., the unification of the nation, by liberating the territories inhabited by Romanians, which today are embedded in the Austrian-Hungary monarchy"* (Ministry of National Defence, 1934, p. 97).

The strategic goal of the war was to defeat the enemy in Transylvania, and thus to control the Hungarian Plain, the Tisza and Danube Valleys. For the four armies, offensive actions were planned in Transylvania, Banat and Hungary (Northern Army, 1st and 2nd Armies) and defence in the south (3rd Army), followed by a Romanian-Russian offensive after 10 days (Cupșa, 1967, p. 34).

Some military leaders, including General Alexandru Averescu, Russian General Mihail Alekseev, head of the Russian General Headquarters and French General Joseph Joffre, commander of the French Army, considered the execution of the defence to the north and northwest, while most of the forces went on the offensive in the south, against Bulgaria (Stănescu, 2004, p. 18). That course of action would most likely have resulted in the following:

- a detailed planning, in cooperation with the Allies, for the execution of a concentric attack by the Franco-British troops from Thessaloniki – the Eastern Army, led by the French General Maurice Sarrail;
- the Bulgarian Army, with a combative capacity equal to the Romanian Army, would have been defeated in a short time, communications between Germany and the Ottoman Empire being interrupted, which would have meant the capitulation of the latter;
- Romania would have continued its supply through Thessaloniki, the long route that crossed the Russian Empire being shortened;
- The Central Powers would have executed the concentration in Transylvania, without the pressure of the Romanian troops, but they would have collided with a well-organized defence in the mountains;
- the Romanian front, with Russian help and the coming of winter, would have represented a difficult obstacle to overcome.

For that course of action, the purpose of the military campaign would no longer have been the reconquest of Romanian land, which constituted, moreover, the justification of the actions against the Austro-Hungarian Empire. All the steps initiated during the years of neutrality, by politicians, were to guarantee the inclusion of all Romanian territories, which also represented the motivation for entering the war.

The offensive action in Transylvania was based on several considerations, among which:

- motivating citizens to fight in a national war;
- establishing the political goal of the war – the liberation of the Romanian territories;
- the condition imposed by the Russians for the acceptance of our country's conditions to enter the war – the Romanian army on the left wing of the Russian armies in Transylvania (Kiriţescu, 1989, p. 569).

The aim of the 1916 military campaign, carried out between August 15/27, 1916-28 December 1916/10 January 1917, was to liberate Transylvania as quickly as possible, before the Central Powers concentrated in the area. The final objectives for the Romanian Army were, in the west, the city of Budapest and in the south, the Balkan Mountains. Although the initial planning emphasized two offensives – one in Transylvania and one in Bulgaria, in cooperation with Russian troops, in reality one offensive and three defensive operations were executed, as follows:

- offensive in Transylvania;
- defence on the southern front;
- defence of passers-by in the Carpathian Mountains;
- defence of the territory of Muntenia.

The mobilization of the Army was ensured by 17 cover groups, made up of 119 battalions and 77 batteries, with an effective number of approximately 135,000 men, deployed in the pass area of the Carpathian Mountains, starting from September 1915 (Romanescu, Tudor, Cucu, Popescu, 1985, p. 77). The action of the cover groups represented a new tactic used by the Romanian Army. According to the existing rules, also adopted by other foreign armies, the cover troops executed the defence, on intermediate alignments, until a final alignment, which was maintained at all costs. The chosen solution, through the campaign plan, created surprise and allowed the main forces to cross the mountains without encountering strong resistance from the enemy (Cupșa, p. 44).

The offensive action in Transylvania was carried out by surprise and led to the advance in the depth of the enemy device:

- • Northern Army: between 50-100 km in the first stage, 50 km in the second stage and 40 km in the last stage, releasing 12,000 km^2;
- 2nd Army: 120 km on the right flank, 70 km in the centre, 90 km on the left flank, releasing 8,000 km;
- 1st Army: approximately 80 km, with three groups of forces along the rivers Olt, Jiu and Cerna (Pavel, Ciobanu, 1993, p. 120).

The defeat following the battle of Turtucaia from August 20-24/ 2-6 September 1916 strongly affected the Romanian Armed Forces, but especially public opinion, which demanded urgent measures to rectify the situation. In the War Council on 2/15 September 1916, two contradictory concepts were stated. General Constantin Prezan demanded the continuation of the initial plan and the liberation of Transylvania, and then the concentration on the southern front. On the other hand, General Alexandru Averescu supported the offensive in the south, a variant that was accepted, being concretized in the Flămânda Manoeuvre.

The change in the conception of the operation, before the troops reached the alignment of the Mureș River, established for the first stage, had dire consequences for the entire front. Achieving this alignment would have shortened the front line, from 800 km to 250 km, which would have allowed the organization of a robust defence, able to withstand a strong enemy (Otu, 2006, pp. 6-20).

At the end of September 1916, the Romanian troops were withdrawn to the Carpathian Mountains, deployed on large fronts, with no possibility of mutual support. The enemy, superior in terms of military equipment and war experience, also benefited from the advantage of the developed communication routes in Transylvania. On the Dobrogea front, the Romanian 3rd Army was disbanded, and the Danube Defence Group was formed in its place (Ib., p. 117).

The stoppage of the German 9th Army in the Carpathian bend, foiled the enemy's plan to separate the Romanian troops and the territory of the country, as well as to conquer, in a short time, the capital. After numerous resistances by the Romanian troops, the enemy managed to break the defence, developing the offensive towards Bucharest, simultaneously with forcing the Danube to the south (Ib., p. 102).

The Romanian General Headquarters decided to neutralize the enemy groups heading towards Bucharest, forming the Prezan Army Group, which, on 17/30 November 1916, attacked the enemy, in the direction of Alexandria-Zimnicea. The attack was not successful because of the action of the German troops in the flank and rear of the Romanian troops, as well as the capture by the enemy of an operation order of General Prezan to the 1st Army (Ib., p. 103). After the unfortunate outcome of the battle for Bucharest, from Argeș-Neajlov, which ended on 20 November/3 December 1916, the Romanian Army began its retreat to the east, up to the alignment delimited by Șușiței, Putna and Siretului Valleys, where the front stabilized, starting from 28 December 1916/10 January 1917. In Moldova, the only unoccupied Romanian territory, withdrew the Royal Family, the Parliament, the Government, the political class and the central administrative institutions.

The halting of the advance of the Central Powers' troops, in the winter of 1916, led German general Erich Ludendorf, the head of the German General Headquarters, to state that: *"we beat the Romanian army but we could not destroy it. We achieved the results that were possible to achieve, but we also had to leave in Dobrogea and Wallachia forces that before Romania's entry into the war we used on the eastern and western fronts or even in Macedonia. Despite the victory obtained against the Romanian army, we were weaker in terms of the general development of the war"* (Muşat, Ardeleanu, 1983, p. 508).

The result of the 1916 campaign is highlighted by the future Marshal Ion Antonescu, then an officer in the Operations Bureau of the General Headquarters, as follows: *"in four months we had lost: morale and momentum, three quarters of the country; the capital, most of our national wealth – oil, cattle and grain stores – and 400,000 people – 100,000 prisoners, 150,000 dead and wounded left in enemy hands and 150,000 wounded evacuated to Moldavia – from the 650,000 who formed the operations armies"* (Antonescu, 1991, p. 24).

In the winter of 1916, the countries of the Balkans, affiliated to the Entente, whose action could create decisive effects on the Eastern Front, were unable to achieve them. Romania and Serbia were taken out of the fight, and Greece neutralized. In addition, the Central Powers benefited from two important resources for the continuation of the war, oil and wheat, both provided by the Romanian territory, because, as the Prime Minister of the United Kingdom, David Lloyd George, stated, in Romania were located *"the richest oil wells from Europe"* (Preda, Pâslaru, Georgescu, Stănescu, 1996, p. 260).

LESSONS LEARNED AFTER THE MILITARY CAMPAIGN OF 1916

After the military actions of our country in the Great War, the answers to the questions: *What went well and why?*, *What did not go well and why?*, *What needs to be done differently?*, will provide solutions for developing lessons learned.

Analysing the main causes of the defeat in 1916, as presented by different historians and military analysts, but also by those directly involved in the conflict, the following can be listed:

- the unfavourable moment chosen for entering the war;
- strategic and tactical errors (offensive actions on two fronts, stopping the offensive in Transylvania, inconsistency in the pursuit of goals, frequent reorganizations of structures, lack of coordination at the central level);
- inadequate preparation of the armed forces and the country for the war (poor provision of equipment, inadequate training, insufficient staffing

of units, low experience of commanders and troops, rivalries between high-ranking commanders);
- non-fulfilment, by the Allies, of some conditions established by the Military Convention (the inaction of the Salonika Army, the low involvement of the Russian Army, the lack of provision of armaments and ammunition).

The unfavourable moment chosen for entering the war.

At the outbreak of the First World War, Romania was caught in a *vise*: to the west in a possible war with the Austro-Hungarian Empire, from which it wanted the annexation of Transylvania, and to the east in a possible conflict with Russia, for the annexation of Bessarabia. Neutrality was a temporary solution, for diplomatic and military preparations, in order to join one of the two military blocs – the Triple Entente/Entente or the Triple Alliance/Central Powers.

Starting from June 1916, with the launch of the Entente offensive on the Western Front, Romania became the target of pressure from the European powers, for its rapid involvement in the war. General Mihail Alekseev, the head of the Russian Army's General Staff, and General Joseph Joffre, the commander-in-chief of the French Armies, asked Romania to enter the war *"now or never"* (Pavel, Ciobanu, 1993, p. 107). This ultimatum is supported by a revelation by Constantin I. Diamandy, minister plenipotentiary at the Romanian embassy in Petrograd, from a secret document between France and Russia, which shows that, after the battles of the Somme and Verdun, the French armed forces *"no longer had breath"* and made a *"warm appeal"* to Russia to *"give in to Romania's demands"* (Preda et al., p. 170). As Constantin Kiriţescu appreciated, Romania entered the war *"not at the favourable moment, freely chosen by us, but at the one imposed by the Allies, to ease the general situation on the European fronts"*. Perhaps even more relevant is the statement of the French General Joffre regarding the involvement of our country in the war: *"it is essential that Romania enters the war, what will happen later, we will see"* (Kiriţescu, 1989, p. 565).

In Europe, the year 1916 was marked by four major events: the Allied offensive on the Somme, the Brusilov offensive, the Italian offensive and the Romanian offensive. French General Joseph Joffre believed that if those four actions had been coordinated, would have had significant effects on the Central Powers. Most likely, a joint action plan would have made Romania's entry into the war a valuable strategic moment. At the same time, the fears of Prime Minister Ion I.C. Brătianu regarding Russia's opposition to Romania's demands and actions had the effect of delaying the signing of the Convention with the Entente. Now that we know exactly the reality of the facts and especially how Russia was carrying out its tasks, we can give

credit to the Prime Minister in his actions for ensuring the requirements for entry into the war.

Sir Winston Churchill stated that the most favourable moment, for Romania's entry into the war, was when the Brusilov offensive was advancing in Galicia and *"if the mobilization of the Romanian Army had occurred towards 10 June, a significant number of units could have entered the campaign before the end of the month (...). This event (...) might have decided the fate of the campaign"* (Preda et al., pp. 66-67). Basically, six weeks were lost, during which the Russian offensive decreased in intensity. Compared to the promised offensive of the Thessaloniki Army, for the support of the entry of the Romanian Armed Forces into the war, the Brusilov offensive would have represented a more credible condition, for the Entente to have tried to attract Romania to its side. Even under those conditions, Romania would probably have hesitated, because it had not yet received the requested war materials, in sufficient quantities, nor did it have definite assurances regarding the support of Russian troops in Dobrogea.

At the time of Romania's entry into the war, the Allies' offensives on the other fronts had stopped, and there were no longer the resources needed to carry out large-scale actions. The Germans had previously moved their troops from Verdun to stop the Allied offensives on the Somme and the Eastern Front. After Romania's entry into the war, the reorganization and merger of powerful troops of the Central Powers took place on the Transylvanian front, gradually forming the Archduke Carol Army Group, from the German 9th Army (General Erik von Falkenhayn, former head of the German General Headquarters) and the 1st Austro-Hungarian Army, as well as some structures within the 7th Austro-Hungarian Army.

Strategic and tactical errors

At the strategic level, the war was fought in two directions, without benefiting from conclusive support from the Allies. The Romanian armed forces had to fight on a front of 1,400 km, representing over 75% of the total length of the borders. The campaign plan of the Romanian Armed Forces was *"in accordance with the political-military goals proposed, it allowed the solution of some particularly complex strategic situations and was in agreement with the situation in which Romania and the Romanian Armed Forces were at that time, as well as with the provisions of the Treaty of Alliance of August 1916 concluded with the Entente countries"*. The division of forces for the offensive was judiciously planned, considering the fact that the enemy did not have important troops on the Carpathian border in August 1916 (Toma, Boaru, 2018, p. 78).

The lack of reserve in the first stage, created difficulties for covering some breaches, replacing some forces or strengthening some intensively attacked areas. On 1/14 October 1916, the reserves of the 2nd and Northern Armies were formed, and on 9/22 October 1916, after the Dobrogea front was pushed back, the French General Henry Mathias Berthelot insisted on the creation of reserves (Ib., p. 138).

There was not a very good coordination of the large units, by the General Headquarters. An example in this regard was the withdrawal of the Northern Army, although it had accomplished its mission. Most likely a variant attack on the flank and rear of the German 9th Army would have been preferable to retreat. The action of the 2nd Army was also not coordinated with the manoeuvres of the 1st Army, because the overall picture regarding the disposition of the troops was not known (Ib., p. 157). The General Headquarters planned the manoeuvre on the right flank with the Northern Army, while the 1st Army did not constitute a solid pivot and did not act decisively, for the occupation of the Mureș Valley, which would have led to the return of the devices of the German 9th Army and the Austro-Hungarian 1st Army. In the battle for Sibiu, decision and action were lacking, and the city was not occupied by Romanian troops (Pavel, Ciobanu, pp. 126-127). The front line, in the form of a circular arc, favoured the Romanian troops on the offensive, because the Austro-Hungarian units were advanced, with the tip in the Bârsei Plain. The necessary conditions existed, with the help of the relief of the area, for a double enveloping manoeuvre, executed with the Northern Army and the 1st Army, which would have caught the enemy in a pincer. In addition, the links between the commands, even after three months of war, functioned with difficulty, and the subordinates did not report to the higher commands the situation on the ground, with *"all the prescriptions of the regulations"* (Rosetti, 1997, p. 153).

On the southern front, instead of defending the bridgeheads in the Dobrogea area, General Gheorghe Dabija, participating in the Great War as commander of the 6th Infantry Regiment *"Mihai Viteazul"* and chief of staff of the 3rd Army, proposed *"the withdrawal of the 17th Division from Turtucaia and even the 9th Division from Silistra and the concentration of the three divisions and the Russian Group north of Silistra, which would have constituted a compact mass with the possibilities of manoeuvre and an undeniable increase in combat power"* (Moise, 2000, p. 273). A variant of action was proposed by the Russian General Mihail Alekseev, the redeployment of four divisions on the western front, for the creation of a manoeuvre group of eight divisions in the Bazargic-Silistra area and the continuation of the offensive in Transylvania, with the Army of the North and the Romanian 2nd Army, because the enemy had not finished mobilizing. This option had some weak points,

because a division was to defend a front of 15-20 km, in a plain area, with great shortages in artillery and automatic weapons (Protopopescu, 1970, p. 385).

In order to fulfil the major goals of the 1916 plan of operations, one of the most viable options would have been the withdrawal of the defence from Dobrogea along an alignment to the north, to protect the Cernavodă-Constanța road, the evacuation of the troops from Turtucaia and Silistra, at the same time with the execution of the offensive in Transylvania, up to the alignment of the Apuseni Mountains or Mureș-Târnava Mare (Ib.). Thus, the forces were concentrated on the main direction of action to the west, and in the southern area, a strong defence, on an alignment well prepared in time, would have supported the offensive operation and would have prohibited the penetration of the enemy to the north.

Regarding the offensive in Transylvania, the French Marshal Joseph Joffre considered that the results achieved should be preserved, the defence organized and, only then, the troops deployed to the southern border, which, together with the Russian ones, should attack the Bulgarians, in order to achieve the junction with the Army of the East. He stated that *"as a result of the fact that it had not been executed in time and with sufficient energy, the advance of the Romanian armed forces in Transylvania fell into the void and the decisive manoeuvre against the Austrian armed forces seemed lost"* (Preda et al., p. 238).

Stopping the offensive in Transylvania, a controversial decision, was taken after the failure at Turtucaia, under the pressure of the whole society. It later turned out to be a wrong decision that caused chain reactions, radically changing the course of action, which was proceeding according to the originally established plan. Basically, two successive offensives were planned, which were intended to be strong and decisive, for which the Romanian Armed Forces did not have the necessary resources and depended on two external factors: Russian support on the Dobrogea front and the action of the Thessaloniki Army (Cupșa, p. 181).

At the operational level, in defence, the combat units were formed as a single echelon, with a division-level reserve, being grouped on the main directions of denial, but separated by large intervals, due to the length of the front. Romanian troops executed manoeuvres and counterattacks, and when the defence benefited from natural obstacles, the enemy was successfully repulsed. Offensive countermeasures to restore the previous limit of the defence or to destroy the enemy penetrated inside the defence, attacking one or both of its flanks, were executed with the troops in reserve, regrouped or received as reinforcement. As part of the offensive countermeasures, envelopments and returns were executed, the offensive return being often adopted, in which all the forces of the large unit took part (Ib., p. 196).

At the tactical level, the 1916 campaign was dominated by the execution of defensive operations by the large units and units of the Romanian Armed Forces, although initially, the planning was based on the offensive.

An optimal defence device for a division, it had a front of 10-15 km. In reality, the combat actions of the divisions were executed on wide fronts, 20 km in defence, 10-15 km in offensive. Thus, the combat units did not ensure the concentration of troops on the main directions to be prohibited, a larger number of subunits being required to cover the entire area of operations, which led to the impossibility of creating strong reserves. The infantry division had in reserve one, at most two infantry battalions, out of the total of 20 battalions. The reserves were located in areas close to the defence limit, being made up of units with elderly people, equipped with old weapons (Ib., pp. 184-188). They were easily engaged by the enemy and brought into battle earlier, unable to be used in the decisive moments.

In the defensive, the advance limit was usually chosen on the military ridge of the mountain peaks, to ensure the conditions of observation and firing. The next line of defence was set up on the counter-slope, where the reserves were also disposed, being very difficult to hit by the enemy. The artillery occupied firing positions to the side, for flank firings (Ib., p. 193). In some situations, defence was also adopted at the foot of the mountains or at the exit of the mountain massif.

In offensive were several detachments, with a different structure, which executed independent missions. Within the large unit, the detachments were decentralized, being supported by the action of the reserve, consisting of 1-3 infantry battalions and an artillery battery. Each detachment had a vanguard, made up of a third of the total forces, as well as interspersed artillery (Ib., p. 190).

Inadequate preparation of the armed forces and the country for the war

The deficiencies in the field of equipping and training the troops could not be covered during the years of neutrality, related to the scale of the military actions carried out on the two fronts and the experience of the two years of war of the enemy (Prisăcaru, 2016, pp. 238-260).

The participation of the Romanian armed forces in the Second Balkan War in 1913 demonstrated the major shortcomings and raised an alarm signal to the Liberal Government installed at the beginning of 1914. Prime Minister Ion. I. C. Brătianu, who also ensured the portfolio of the Ministry of War, in cooperation with the General Staff, developed a series of plans, aimed at easing the shortages of goods and providing the Romanian Armed Forces with the appropriate equipment. Important sums of money had been allocated, both from the state budget and from external credits.

Romania's situation at the beginning of the war was not very good, in terms of industry and economy. Heavy and machine-producing industries were almost non-existent, and food industry was not developed. Therefore, defence industry did not offer the required products, most of the armaments and ammunition being imported from Germany and the Austro-Hungarian Empire. In August 1916, the national defence industry produced *"two projectiles for each cannon and one cartridge for each infantry weapon per day"* (Cupșa, p. 22). If a machine gun had an average rate of fire of 500 shots/minute, it is easy to see the degree of ammo insurance.

The outbreak of the war determined the blocking of some orders and military equipment contracts, by the belligerent states, as a result of the Romanian Government's lack of decision regarding the choice of an alliance, as well of means to meet own needs. To cover some deficiencies, compromise solutions were adopted, by using new ammunition for old artillery pieces, transforming fortification artillery into field artillery and reprofiling some civilian factories (Pașcu, 1988, p. 123). The Romanian infantry had modern but insufficient weapons and the reserve units were equipped with old weapons. While a Romanian battalion had 1-2 automatic weapons, a German or Austrian battalion had 5-6 heavy machine guns and 9 light machine guns (Cupșa, p. 28).

Both the lack of a national defence industry and the decrease in the import of military equipment could be mitigated by a long-term plan of arms and ammunition purchases, so as to achieve the appropriate equipment for the units. The lack of such a plan led to the diversified acquisition of military equipment, as a last resort. It should also be taken into account that the signing of the defensive convention with the Central Powers in 1883 put our country at risk from the east, but also created a dependence on imports of military equipment.

Numerous units were created to meet the quantitative criteria, but without being properly equipped and trained. From 15 divisions in 1914, 23 divisions were mobilized, through the use of poorly staffed and prepared units, which decreased the combative capacity as a whole (Kirițescu, p. 578). The staff of the Romanian Armed Forces was insufficient, because not enough military officers were trained during peacetime. Thus, in a division with an actual strength of 27,000 soldiers, instead of 2,000 officers, were assigned 640 officers. In addition, many structures were made up of reservists, with poor military training (Cupșa, ib.).

When Romania entered the war, there was a lack of homogeneity of the units because *"new units were created by diluting the existing ones; and on the other*

hand, confusing the coverage of the mobilization and the concentration with the actual operations, the units were amalgamated" (Averescu, 1935, p. 18). An example in this regard was the disorganization at the command of the 1st Army, reported on 28 October/10 November 1916, as a result of forced changes of army, corps and division commanders (Rosetti, p. 146).

Terrain works for defence followed the provisions of the operations plans, which were permanently modified, depending on the evolution of international events. At the beginning of the 20th century, works were carried out on the fortified areas of Turtucaia, Silistra and Bazargic, three successive defence alignments were prepared in Dobrogea, resistance centres, firing ditches, shelters, command points, firing positions for artillery were built, wire nets, a dam of approximately 90 Hertz type mines was placed for the defence of Constanța port and sapper dams were created in the main passes of the Carpathian Mountains (Croitoru, 2015, pp. 35-45).

However, the measures for the preparation of the territory were not sufficient to ensure a strong defence. As stated by General Traian Moșoiu, the commander of the 23rd Infantry Division, the Romanian Army stayed *"for almost a month in the greatest passivity, waiting for the enemy to impose its actions on us"*. Strengthening the defence positions *"with all the fighting means of a modern army"* would have created major advantages and would have strengthened the defence of the Carpathians (Moșoiu, 1987, p. 97). Russian General Aleksei Alexeevici Brusilov, the commander of the Russian 8th Army, in a dialogue with General Ion Rașcu, the commander of the Group of 9th and 19th Divisions in Dobrogea, considered that the Romanian armed forces were defeated in 1916, because they had not prepared *"in advance positions reinforced in all directions of attack, because of which we lost so much territory in such a short time"* (Dumitrescu, 2008, p. 181).

Non-fulfilment, by the Allies, of some conditions established by the Military Convention

The mobilization and concentration of the Romanian Armed Forces were to be supported by the offensive actions of the Russian Empire in Bucovina and of the Army of the East against the Bulgarian troops. Russia undertook to send two infantry and one cavalry divisions to the Dobrogea front against the Bulgarian armed forces and to act with the Black Sea Fleet to prevent any attempt of the enemy to land on Romanian territory (Cupșa, p. 21). The Allies recognized the *"organizational and command independence of the Romanian Armed Forces"* and obliged themselves to deliver, against cost, munitions and war material, within the limit of 300 tons per day (Milea, 1987, pp. 149-151).

There have been some theories about the real intention of the Entente to draw our country into the war, to polarize some of the enemy's forces, in order to depressurize their own forces on other fronts, especially on the western front. Glenn E. Torrey claims in his work, regarding our country's participation in the war, that *"Romania's defeat was a predictable fact for those who knew the strategically vulnerable geographical position of the country, the poorly trained and poorly equipped army, the incompetence of the high command and the dubious promises of support made by its allies. There is no doubt that the British military attaché was thinking of these factors when he confessed, with a heavy conscience, to his French colleague shortly after they signed the military convention: <I feel like a hired assassin>"*(Torrey, 2014, p. 349).

Unfortunately, the commitments made by the Allies regarding Romania were not respected in their entirety, but in essential parts. The offensive of the Russian Army in Bucovina was not executed, nor that of the Thessaloniki Army, in support of the action of the Romanian Army. The Brusilov Offensive, executed on 22 May / 4 June 1916, had an initial success that led the Central Powers to deploy 26 German, 7 Austrian, and 2 Turkish divisions in Galicia and Bucovina. The troops brought in to support it stopped the Russian offensive, counterbalancing the balance of forces (Moise, 2000, p. 270). Therefore, a subsequent action in the same area could hardly be expected to have the same effect as the initial one, given the fact that the defences had been reinforced with additional troops.

Regarding the support of the Russian Empire, there were inconsistencies between the measures assumed by the Military Convention and those executed. Mainly, the Russian military leaders believed that Romania should defend itself on the Siret, therefore they delayed sending troops and cited the lack of adequate railway infrastructure to ensure the transport of units and supplies to Romanian territory. The Russian General Mihail Alekseev declared, in January 1916, that he could support Romania with an army consisting of 10 divisions and would launch an offensive in the northwest, to allow the action of the Romanian forces in Transylvania (Atanasiu, Iordache, Iosa, Oprea, Oprescu, 1979, p. 121). On the other hand, the Russians did not support Romania, considering that it had time *"during a period of two years of neutrality, to organize itself from a military point of view"* (Preda et al., p. 376).

Russian troops were sometimes lacking in energetic action, arriving late in the action areas, not achieving a concentration of forces, acting in directions other than those indicated, or invoking various reasons for not participating in the battle.

Armament deliveries to Romania were obstructed by the Russian Empire, so that the Romanian Armed Forces would not become too strong. Russia's support was granted when its own territory was threatened, and the alliance with Romania had as its main objective the elimination of a regional adversary – the Austro-Hungarian Empire. Russian historians considered that a neutral Romania, which would guarantee the left flank of the Tsarist Army, would have been more beneficial than an allied Romania which would badly guard an extended front (Kiriţescu, p. 575).

There were about 400,000 forces in Thessaloniki – French, British, Serbian, Italian and Russian ones. The numbers regarding the composition of the Army of the East, as this grouping was also called, have undergone numerous changes, depending on the cited sources – the report of a French official presents a number of 127,000 combatants, instead of 307,000 as presented by the French General Headquarters (Ib., p. 568). Romania's request was that this army launch the offensive, as far as possible, 15 days before its entry into the war. The French General Maurice-Paul-Emanuel Sarrail, the commander of the Army of Thessaloniki, also called the Army of the East, received orders from General Joseph Joffre, to carry out the attack, with all forces, on the Greek border and to pursue the enemy in the general direction of Sofia. The British Government, however, did not trust the actions of General Sarrail, due to some difficulties that did not guarantee success: the lack of the necessary forces to attack such an extended front, the difficult establishment of links between the component nations, the lack of heavy artillery and the weakening of the left flank through the presence of Serbian soldiers (Preda et al., p. 68).

The actions of the Army of the East, as originally planned, had some objectives: striking the Bulgarian forces in southern Macedonia to cover the mobilization and concentration of the Romanian Army, continuing the offensive and destroying the enemy from deep, simultaneously with the attack of the Romanian troops south of the Danube. Although it was planned 8 days before our country's entry into the war, General Sarrail offensive was not possible due to the attack of the Bulgarian Army on both flanks of the Thessaloniki front and the non-involvement of the British Army, which conditioned the action on Romania's declaration of war against Bulgaria. After Muntenia was conquered and the withdrawal to Moldova took place, the Thessaloniki Army offensive to support Romania ended, and General Sarrail was ordered to execute a defensive operation to defend the reconquered territory (Moise, p. 344).

CONCLUSIONS

The two years of neutrality, although they improved, quantitatively and qualitatively, the country's readiness for war, represented a period when the enemy strengthened and gained experience on the battlefield too. These attributes, along with the use of all categories of weaponry and the application of tactics practiced in battle, represented assets successfully used by the Central Powers on the Romanian front. The initial success of the Romanian troops, from August 1916, created the conditions for the continuation of the offensive, but the lack of organization and the shortages of armaments and ammunition, as well as the non-fulfilment by the Allies of the obligations assumed by the Military Convention, stopped the actions and gave Germany and Austria-Hungary the possibility to organize their troops.

Although approximately 3/4 of the country's territory was conquered, the Central Powers failed to achieve their initial goal – eliminating Romania from the war. The withdrawal to Moldova led to saving the existence of the Romanian state, but also to preserving the governing authorities that made decisions for an independent and sovereign state. Strategically, the Romanian Armed Forces saved themselves, managing to resist in the face of a superior enemy. Within the Alliance, Romania managed to polarize an important number of units and large units of the Central Powers, releasing the pressure from other areas of the European front.

Participation of the entire nation in the war effort

Until the execution of the actual military action, measures were in place to prepare and support the armed forces, the political class and the entire society. Mobilization involves the participation of both active and reserve personnel who have undergone various forms of military training and are fit to be combatants. The preparation of the territory and the economy for defence, as well as the transition from peace production to war production, involves the activity of an important part of society, which operates in certain fields – industry, agriculture, construction, transport etc. In the event of a conflict, the armed forces represent the spearhead, having the support of the entire society behind, for the joint effort to defend sovereignty, territorial integrity and independence. It is also necessary to develop a national defence industry and stockpiles of essential raw materials.

Coordination between the politico-military objective of the war and the resources available

As we well known, the military implements political decisions, therefore there must be unity of effort and thought between the political and the military leadership.

The campaign plan was based on the political objective – the achievement of the unitary state, objective for which military actions were planned. Therefore, the right character of participation in the war was represented by the liberation of the territories inhabited by the Romanian population from Transylvania, this being also a moral element, motivating the population, which wanted the unification with the brothers over the mountains. The allocation of forces, following mobilization, should be appropriate and take into account the terrain conditions and the enemy's capabilities. The Romanian armed forces, instead, created numerous units, which could not be adequately equipped.

Achieving surprise

The essence of the initial action of the Romanian troops was not to achieve surprise, but rather to sustain it, until the time or place that allowed the conditions for a strong resistance against the enemy. The defeat at Turtucaia put an end to the momentum of the attack, before the troops occupied a strong alignment in the field – the Mureș River or the Apuseni Mountains. The resumption of the offensive in Transylvania, after the failure of the Flămânda Manoeuvre, offered the enemy the opportunity to gain time, to organize the forces. The defeat at Turtucaia should not have affected the offensive in the west, which was being carried out successfully. In addition, 3 armies separated by mountains operated in Transylvania, with limited possibilities for coordination, and the shortening of the front line would have provided the necessary conditions for a robust defence.

The superiority of a force lies in good organization, training and leadership

With painful consequences, the military campaign of 1916 brought to the Romanian armed forces a rich experience of war, materialized through adaptations of techniques, tactics and procedures of fighting and the use of the armament. If in August 1916, we were talking about the war experience of the enemy, in December we can discuss about a war experience of the Romanian troops. At the beginning of the war, the organization of the Romanian armed forces was similar to the European armed forces – army, corps and division echelons, and the infantry was used in a greater proportion, to the detriment of the artillery. The Army Group was used to carry out large-scale actions, but strong reserves were not established from the beginning to deal with unexpected situations.

Development of national defence industry

From the equipment point of view, the Romanian Armed Forces had numerous shortages, given the lack of domestic production, but also the failure of the Allies to supply military equipment in the agreed quantities. The development of the national defence industry is important for two reasons: ensuring the necessary equipment and independence from imports. The military campaign of 1916 highlighted, through the shortages recorded by the Romanian troops, the need for a good supply of aircraft, anti-aircraft artillery, communications and engineering equipment.

Behaviour in extreme situations

The task of finding guilty persons for the failure of the 1916 military campaign is difficult. There is no doubt that certain behaviours of some soldiers – lack of initiative, preparation, failure to follow orders, leaving the battlefield, desertion – are to be condemned and, in some moments, they decided the outcome of the battle. On the other hand, the actions of some commanders who executed frontal strikes, envelopments, infiltrations and actions by surprise with the aim of defeating the enemy must also be taken into account. Without these actions, a resistance of the Romanian troops would not have been possible until December 1916, nor would the numerous actions that led to the enemy's halt.

BIBLIOGRAPHY:

1. Antonescu, I. (1991). *Românii. Originea, trecutul, sacrificiile şi drepturile lor*. Iași: Editura Moldova.
2. Atanasiu, V., Iordache, A., Iosa, M., Oprea, I., Oprescu, P. (1987). *România în anii Primului Război Mondial*, vol. 1. București: Editura Militară.
3. Averescu, A. (1935). *Notițe zilnice din război (1916-1918),* 2nd ed., Bucureşti.
4. Croitoru, M.C. (2015). *Pregătirea pentru apărare a economiei, teritoriului și populației (1877-1939)*, in *"Document: Buletinul Arhivelor Militare Române"*, XVIII, no. 4 (70), București.
5. Cupșa, I. (1967). *Armata română în campaniile din anii 1916, 1917*. București: Editura Militară.
6. Dumitrescu, H. (2008). *Figuri de comandanți din Primul Război Mondial în Jurnalul de front al generalului Ion Raşcu*, in *"Cronica Vrancei"*, no. VII. Focșani: Muzeul Vrancei
7. Joint Publication (AJP)-3(C) (2019). *Allied Joint Doctrine for the Conduct of Operations*. Edition C. Version 1. NATO Standardization Office (NSO).
8. Kiriţescu, C. (1989). *Istoria războiului pentru întregirea României*, vol. I. Bucureşti: Editura Ştiinţifică şi Enciclopedică.
9. Milea, V. (1987). *România în anii Primului Război Mondial*, vol. I. București: Editura Militară.

10. Moise, L. (2000). *Importanța frontului de sud în planul de campanie adoptat la intrarea României în Primul Război Mondial*, in *"Revista Analele Dobrogei"*, year IV, no. 1. Constanța: Editura Muzeului de Istorie Naţională şi Arheologie.
11. Moșoiu, T. (1987). *Memorial de război (august-octombrie 1916)*. Cluj-Napoca: Editura Dacia.
12. Muşat, M., Ardeleanu I. (1983). *De la statul geto-dac la statul român unitar*. Bucureşti: Editura Ştiinţifică şi Enciclopedică.
13. Otu, P. (2006). *Turtucaia. Sfârșitul iluziilor. Începutul dezastrului*, in *"Document: Buletinul Arhivelor Militare Române"*, IX, no. 1-4 (31-34), București.
14. Pașcu, Ș. (1988). *Istoria militară a poporului român*, vol. V. București: Editura Militară.
15. Pavel, T., Ciobanu N. (1993). *Armata română și Marea Unire, contribuții la realizarea Unirii și la consolidarea statului național*. Cluj-Napoca: Editura Daco-Press.
16. Preda, D., Pâslaru, Ș., Georgescu, M., Stănescu, M. (1996). *România în timpul Primului Război Mondial – Mărturii documentare, vol. I (1914-1916)*. București: Editura Militară.
17. Prisăcaru, D. (2016). *Starea armatei României la declanșarea Primului Război Mondial. Cauze și determinări pentru adoptarea neutralității armate în perioada 21 iulie/3 august 1914-4/17 august 1916*, in *"Acta Moldaviae Meridionalis: ActaMM"*, XXXVII. Vaslui: Editura Pim.
18. Protopopescu, G. (1970). *Mari comandanți români în Primul Război Mondial*, in *"Acta Mvsei Napocensis"*, no. VII. Cluj-Napoca: Muzeul de Istorie.
19. Romanescu, Gh., Tudor Gh., Cucu, M., Popescu I. (1_985). *Istoria infanteriei române II*. București: Editura Științifică și Enciclopedică.
20. Rosetti, R.R. (1997). *Mărturisiri (1914-1919)*, editor, foreword and notes Maria Georgescu. București: Editura Modelism.
21. Stănescu, M. (2004). *Turtucaia în viziunea unui ofițer german*, in *"Document: Buletinul Arhivelor Militare"*, VI, no. 2-3 (24-25). București.
22. The NATO Lessons Learned Handbook (2022). Fourth Edition, Joint Analysis and Lessons Learned Centre.
23. Toma, Gh., Boaru, Gh., (2018). *Planurile de campanie și gândirea strategică românească în Primul Război Mondial. Concluzii şi învățăminte pentru arta militară românească*, in *"Revista Academiei de Științe ale Securității Naționale"*, no. 1. București: Editura Sitech.
24. Torrey, G.E. (2014). *România în Primul Război Mondial*. Bucureşti: Editura Meteor Publishing.


RMT



Order *"Meritul Cultural"*
in the rank of *"Knight"*, F Category
– *"Promotion of Culture"*
(Presidential Decree no. 646
on 24.08.2004)



Order *"Meritul Cultural"*
in the rank of *"Officer"*, F Category
– *"Promotion of Culture"*
(Presidential Decree no. 483
on 30.06.2014)



Order *"Meritul Cultural"*
in the rank of *"Comandor"*, F Category
– *"Promotion of Culture"*
(Presidential Decree no. 483
on 10.05.2023)





gmr.mapn.ro
facebook.com/gmr.mapn.ro