



ROMANIAN MILITARY THINKING



ERIH PLUS
EUROPEAN REFERENCE INDEX FOR THE
HUMANITIES AND SOCIAL SCIENCES

INDEX COPERNICUS
INTERNATIONAL

DOAJ

E3
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 CONFERENCE PROCEEDINGS



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

NOVEMBER 2025
BUCHAREST

7TH EDITION



PUBLISHER THE DEFENCE STAFF

ORGANISING COMMITTEE

Chairman:

Lieutenant General Dragoş-Dumitru IACOB

Vice-Chairmans:

Lieutenant General Iulian BERDILĂ

Major General Valentin BRÎNZEI

Members:

Lieutenant General Ciprian-Constantin NAN

Major General Mircea GOLOGAN

Major General Adrian BRÂNĂ

Major General Iulian DANILIU

Brigadier General Cornel-Traian SCURT

Brigadier General Nelu-Gabriel BOŢOG

Brigadier General Ilie-Marian DRAGOMIR

Brigadier General Cornel-Tonea BĂLAN

Colonel Daniel ȚIGĂNUȘ

Lieutenant General Ciprian MARIN

Vice Admiral Mihai PANAIT

Lieutenant General Leonard-Gabriel BARABOI

Major General Eugen MAVRIȘ

Brigadier General Constantin VIZITIU

Brigadier General Marius ȘERBESZKI

Rear Admiral (LH) Alecu TOMA

Colonel Dorel BADEA

Secretariat:

Colonel Cristian-Mihai CHIOREAN

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".

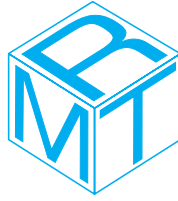
*Carol – King of Romania
Issued in București on 8 December 1897*



Printed

at Military Technical Publishing Centre

C ___/___ B 885/24.12.2025



**ROMANIAN MILITARY THINKING CONFERENCE
PROCEEDINGS**

***STRATEGIC RESILIENCE
AND NATIONAL DEFENCE
– FROM PLANNING TO ACTION
IN THE FACE OF HYBRID THREATS –***

7TH EDITION

**Print: ISSN 2668-7984, ISSN-L 2668-7984
Online: ISSN 2668-8115, ISSN-L 2668-7984
DOI: 10.55535/RMT.2025.3**

Romanian Military Thinking Journal is included in the Journal Master List of the **ERIH PLUS, INDEX COPERNICUS INTERNATIONAL, DOAJ, CEEOL, MIAR, EBSCO's** and **ROAD Catalogue**

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 2025

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

Brigadier General 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

Mirosław SMOLAREK,

“General Tadeusz Kosciuszko” Land Forces
Academy, Wrocław, Poland

Dariusz SKORUPKA,

“General Tadeusz Kosciuszko” Land Forces
Academy, Wrocław, Poland

Karl PRONHAGL,

Theresian Military Academy, Wiener
Neustadt, Austria

Árpád POHL,

Faculty of Military Science and Officer
Training, Budapest, Hungary

Colonel Assoc. Prof. Dr. Harald GELL,

Chairman of EU Military Erasmus
Programme, Theresian Military Academy,
Austria (expertise: military education and
training)

Captain (Ret TR Navy)

Assoc. Prof. Dr. Taner ALBAYRAK,

Piri Reis University, Istanbul, Türkiye
(expertise: maritime security, strategy and
geopolitics at the Black Sea)

Dr. Bonita JACOBS,

University of North Georgia, Atlanta, USA

Prof. Stefano GEUNA,

Universita Degli Studi di Torino, Torino, Italy

Prof. Dr. Jaromir MARES,

Brno, the Czech Republic

Prof. Dr. Pavel OTRISAL,

Brno, the Czech Republic

Assoc. Prof. Dipl. Jozef PUTTERA, BEng,

CSc, Armed Forces Academy
of “General Milan Rastislav Stefanik”,
Liptovsky Mikulas, Slovakia

Assist. Prof. Dr. Antonia COLIBĂȘANU,

Department of International Relations
and European Integration, National
School of Political Studies and Public
Administration, Romania

Dr. Larry WHITE,

Lecturer in American and International Law,
University of Economics and Technology,
Ankara, Turkey

Assoc. Prof. Dr. Iulian CHIFU,
“Carol I” National Defence University,
Romania

Assoc. Prof. Dr. Dan-Lucian PETRESCU,
“Carol I” National Defence University,
Romania

Assoc. Prof.
Dr. Ștefan Antonio DAN-ȘUTEU,
“Carol I” National Defence University,
Romania

Prof. Dr. Cristian-Octavian STANCIU,
“Carol I” National Defence University,
Romania

Prof. Dr. Lucian-Valeriu SCIPANOV, BEng,
“Carol I” National Defence University,
Romania

Prof. Dr. Niculai-Tudorel LEHACI,
“Carol I” National Defence University,
Romania

Assoc. Prof. Dr. Daniel ROMAN,
“Carol I” National Defence University,
Romania

Assoc. Prof. Dr. Cristian ICHIMESCU,
“Carol I” National Defence University,
Romania

Assoc. Prof.
Dr. Ciprian PRIPOAE-ȘERBĂNESCU,
“Carol I” National Defence University,
Romania

Assoc. Prof. Dr. Adi MUSTAȚĂ,
“Carol I” National Defence University,
Romania

Assoc. Prof. Dr. Claudiu-Valer NISTORESCU,
“Carol I” National Defence University,
Romania

Assoc. Prof. Dr. George-Ion TOROI,
“Carol I” National Defence University,
Romania

Assoc. Prof. Dr. Ionuț-Cosmin BUȚĂ,
“Carol I” National Defence University,
Romania

Assoc. Prof.
Dr. Florentina-Loredana DRAGOMIR,
“Carol I” National Defence University,
Romania

Assoc. Prof. Dr. Elena ȘUȘNEA,
“Carol I” National Defence University,
Romania

Assoc. Prof.
Dr. Mădălina-Dănuța SCIPANOV,
“Carol I” National Defence University,
Romania

Assoc. Prof. Dr. Mirela IONIȚĂ,
“Carol I” National Defence University,
Romania

Assoc. Prof. Dr. Veronica PĂSTAE,
“Carol I” National Defence University,
Romania

Dr. Senior Instructor Adrian MIREA,
“Carol I” National Defence University,
Romania

Senior Instructor
Dr. Daniela-Elena HRAB,
“Carol I” National Defence University,
Romania

Dr. Florian CÎRCIUMARU,
Director, Centre for Defence and Security
Strategic Studies, “Carol I” National
Defence University, Romania

Scientific Researcher II
Dr. Alexandra SARCINSCHI,
Centre for Defence and Security Strategic
Studies, “Carol I” National Defence
University, Romania

Scientific Researcher II
Dr. Cristian BĂHNĂREANU,
Centre for Defence and Security Strategic
Studies, “Carol I” National Defence
University, Romania

Scientific Researcher II
Dr. Mirela ATANASIU,
Centre for Defence and Security Strategic
Studies, “Carol I” National Defence
University, Romania

Scientific Researcher III Dr. Daniela LICĂ,
Centre for Defence and Security Strategic
Studies, “Carol I” National Defence
University, Romania

Scientific Researcher III
Dr. Crăişor Constantin IONIŢĂ,
Centre for Defence and Security Strategic
Studies, “Carol I” National Defence
University, Romania

Prof. Dr. Aurelian RAŢIU,
“Nicolae Bălcescu” Land Forces Academy,
Romania

Prof. Dr. Dorel BADEA, BEng,
“Nicolae Bălcescu” Land Forces Academy,
Romania

Prof. Dr. Paul TUDORACHE,
“Nicolae Bălcescu” Land Forces Academy,
Romania

Prof. Dr. Dănuţ MOŞTEANU, BEng,
“Nicolae Bălcescu” Land Forces Academy,
Romania

Prof. Dr. Sorin PÎNZARIU,
“Nicolae Bălcescu” Land Forces Academy,
Romania

Prof. Dr. Gheorghe MINCULETE,
“Nicolae Bălcescu” Land Forces Academy,
Romania

Prof. Dr. Toma PLEŞANU, BEng,
“Nicolae Bălcescu” Land Forces Academy,
Romania

Assoc. Prof. Dr. Dumitru IANCU,
“Nicolae Bălcescu” Land Forces Academy,
Romania

Assoc. Prof. Dr. Laviniu BOJOR,
“Nicolae Bălcescu” Land Forces Academy,
Romania

Assoc. Prof. Dr. Alexandru BABOŞ,
“Nicolae Bălcescu” Land Forces Academy,
Romania

Assoc. Prof. Dr. George BUCĂŢA,
“Nicolae Bălcescu” Land Forces Academy,
Romania

Assoc. Prof. Dr. Ioan VIRCA,
“Nicolae Bălcescu” Land Forces Academy,
Romania

Assoc. Prof. Dr. Nicolae MORO,
“Nicolae Bălcescu” Land Forces Academy,
Romania

Assoc. Prof. Dr. Ionuţ Alin CÎRDEI,
“Nicolae Bălcescu” Land Forces Academy,
Romania

Assoc. Prof. Dr. Ioan-Gabriel POPA,
“Nicolae Bălcescu” Land Forces Academy,
Romania

Assoc. Prof. Dr. Romana OANCEA,
“Nicolae Bălcescu” Land Forces Academy,
Romania

Assoc. Prof. Dr. Diana RANF,
“Nicolae Bălcescu” Land Forces Academy,
Romania

Assoc. Prof. Dr. Ştefania BUMBUC,
“Nicolae Bălcescu” Land Forces Academy,
Romania

Assoc. Prof. Dr. Hortensia GORSKI,
“Nicolae Bălcescu” Land Forces Academy,
Romania

Assoc. Prof. Dr. Anca Georgeta DINICU,
“Nicolae Bălcescu” Land Forces Academy,
Romania

Assoc. Prof. Dr. Alina CIUHUREANU,
“Nicolae Bălcescu” Land Forces Academy,
Romania

Assoc. Prof. Dr. Alexandru STOIAN,
“Nicolae Bălcescu” Land Forces Academy,
Romania

Assoc. Prof. Dr. Gabriel MĂNESCU,
“Nicolae Bălcescu” Land Forces Academy,
Romania

Assoc. Prof. Dr. Isabela DRAGOMIR,
“Nicolae Bălcescu” Land Forces Academy,
Romania

Assoc. Prof. Dr. Sabin GUŢAN,
“Nicolae Bălcescu” Land Forces Academy,
Romania

Assoc. Prof.

Dr. Sebastian-Emanuel STAND,
“Nicolae Bălcescu” Land Forces Academy,
Romania

Assoc. Prof. Dr. Constantin ANDREI,
“Nicolae Bălcescu” Land Forces Academy,
Romania

Assoc. Prof. Dr. Brândușa NICULESCU,
“Nicolae Bălcescu” Land Forces Academy,
Romania

Assoc. Prof. Dr. Georgel OPREAN,
“Nicolae Bălcescu” Land Forces Academy,
Romania

Assoc. Prof. Dr. Leontin STANCIU,
“Nicolae Bălcescu” Land Forces Academy,
Romania

Assoc. Prof. Dr. Daniel SOLESCU,
“Nicolae Bălcescu” Land Forces Academy,
Romania

Assist. Prof.

Dr. Elisabeta-Emilia HALMAGHI,
“Nicolae Bălcescu” Land Forces Academy,
Romania

Assist. Prof. Dr. Annamaria SÂRBU,
“Nicolae Bălcescu” Land Forces Academy,
Romania

Assist. Prof. Dr. Tiberiu GIURGIU, BEng,
“Nicolae Bălcescu” Land Forces Academy,
Romania

Assist. Prof.

Dr. Crenguța-Mihaela MACOVEI,
“Nicolae Bălcescu” Land Forces Academy,
Romania

Assist. Prof. Dr. Maria-Lucia RUSU,
“Nicolae Bălcescu” Land Forces Academy,
Romania

Dr. Florin Alexandru PAVEL,
“Nicolae Bălcescu” Land Forces Academy,
Romania

Prof. Dr. Adrian LESENCIUC,
“Henri Coandă” Air Force Academy,
Romania

Assoc. Prof. Dr. Marius MILANDRU,
“Nicolae Bălcescu” Land Forces Academy,
Romania

Assoc. Prof. Dr. Laurian GHERMAN,
“Henri Coandă” Air Force Academy,
Romania

Assoc. Prof.

Dr. Cosmina-Oana ROMAN,
“Henri Coandă” Air Force Academy,
Romania

Assoc. Prof.

Dr. Bogdan-Cezar CHIOSEAUA,
“Henri Coandă” Air Force Academy,
Romania

Assoc. Prof. Dr. Cătălin CIOACĂ,
“Henri Coandă” Air Force Academy,
Romania

Assoc. Prof.

Dr. Daniel-Cornel ȘTEFĂNESCU,
“Henri Coandă” Air Force Academy,
Romania

Assist. Prof. Dr. Rita PALAGHIA,
“Henri Coandă” Air Force Academy,
Romania

Prof. Dr. Ion CHIORCEA,
“Mircea cel Bătrân” Naval Academy,
Romania

Assoc. Prof. Dr. Romeo BOȘNEAGU,
“Mircea cel Bătrân” Naval Academy,
Romania

Assoc. Prof. Dr. Florin NISTOR,
“Mircea cel Bătrân” Naval Academy,
Romania

Assoc. Prof. Dr. Andi Mihail BĂNCILĂ,
“Ferdinand I” Military Technical Academy,
Romania

Dr. Liviu MATACHE,
“Ferdinand I” Military Technical Academy,
Romania

Dr. Valentin-Costinel TOTIR,
Ministry of National Defence, General
Directorate of Human Resource
Management, Romania

Assoc. Prof. Dr. Cristina BOGZEANU,
“Mihai Viteazul” National Intelligence
Academy, Romania

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

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

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

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

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

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

Dr. Manuel STĂNESCU,
Institute for Political Studies of Defence
and Military History, Romania

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

Dr. Sorin CRISTESCU,
Institute for Political Studies of Defence
and Military History, Romania

Dr. Teodora GIURGIU,
National Military Archives of Romania

Dr. Lucian DRĂGHICI,
National Military Archives of Romania

Dr. Iulian BOȚOGHINĂ,
Central Archive Repository,
National Military Archives of Romania

Dr. Cristina CONSTANTIN,
“King Ferdinand I” National Military
Museum, Romania

Dr. Ion RÎȘNOVEANU,
“King Ferdinand I” National Military
Museum, Romania

Dr. Alexandru CRISTIAN,
Joint Forces Command, Romania

Prof. Dr. Silviu NATE,
“Lucian Blaga” University, Romania

Prof. Dr. Cristian BARNA,
University of Bucharest, Romania

Prof. Dr. Ghiță BÂRSAN, BEng,
Romanian Academy of Scientists

Prof. Dr. Florian RĂPAN,
“Dimitrie Cantemir” Christian University,
Romania

Assist. Prof. Dr. Sorina-Georgiana RUSU,
Urban and Landscape Design Department,
“Ion Mincu” University of Architecture
and Urban Planning, Romania

CONTENTS

Cristian-Mihai CHIOREAN	10	Foreword
MILITARY THEORY AND ART		
Ștefan-Claudiu TOPOR	12	Innovative Approaches in Military Leadership at Strategic and Operational Level – Decisive Factor for the Success of Military Actions
Cezar POPA	20	The Architecture of Command-and-Control Systems in Future Military Actions
Romică CERNAT	32	Drones – Weapon Systems with a Growing Role in Military Conflict
Ioan MOLDOVAN	52	Reconfiguring Maritime and River Operations by Using Naval Drones
Florin ȘTEFĂNESCU Dănuț-Gabriel DĂNILĂ Nicolae-Cristian BRÂNZEIU Nelu-Sorin DONEA Paul-Vasile HOSU	72	The Impact of Artificial Intelligence on Contemporary Military Art – Advantage or Vulnerability
Cezar POPA	90	State-of-the-Art Technologies to Be Used in Command-and-Control Systems
Traian OSTAHE	108	Russia's Hobbesian War and Ukraine's Kantian Idea of Universal Peace – Ontological Approaches to the Contemporary Eastern European War Paradigm from an Anthropological Perspective
Romeo BOȘNEAGU	120	Ships Sunk in the Black Sea During the Russian-Ukrainian War (2022-2025) – Lessons for Naval Strategy and Tactics
Marian TĂNASE	138	Multinational Mine Countermeasures Operation in the Black Sea
Marian HOGEA	164	Cognitive Warfare – A New Operational Domain
Daria Ștefania MIHALCEA	178	The Role of the Body in Cognition – Application in Sports and Military Instruction
Marius GHEORGHESCU	186	The New Light Cavalry of the 21 st Century – Analysis of the Innovation and Employment of Motorcycle Assault Groups by the Russian Army in the Ukraine War
INTELLIGENCE AND SECURITY		
Iulian CHIFU	208	Building Up a Prospective Study for The World of Tomorrow
Violeta NICOLESCU	222	The European Union's Strategic Approach to the Black Sea Region – Implications for Regional Security and the Role of Romania

Florentina-Loredana DRAGOMIR	230	Information Intelligence Systems and Machine-Learning Algorithms for Adaptive Decision-Making in the Eastern Security Landscape
Tiberius TOMOIAGĂ	244	Redefining Deterrence: Warfare in the Technological Era
Cătălin-Costel DUMITRIU	260	Emerging Technologies and NATO's Eastern Flank: Perspectives for Romania
Ion CHIORCEA Andrei PAVĂL	276	Methods Used by the Russian Federation to Circumvent International Sanctions Imposed by the International Community
Stayko PROKOPIEV Veselina ALEKSANDROVA Elitsa PAVLOVA Violeta VASILEVA	308	Using Cyber Ranges in Cybersecurity Training as an Action Plan in the Face of Hybrid Threats
Cătălin ANDRUȘ Lucian IVAN	318	Methods Used by the Russian Federation to Circumvent International Sanctions Imposed by the International Community
Georgiana BLĂJAN	336	The Cognitive Component of the Russian Federation's War Against Ukraine
Grudi ANGELOV Stoyan STOYCHEV	352	Demography as an Element that Influences National Power
Adriana SAULIUC	368	Silent Invaders: The Growing Threat of Drones and Balloons
Răzvan CURCULESCU	382	Resilience of Intelligence Services in the Era of Hybrid Warfare
Ana-Raluca STANCU Diana-Cristiana LUPU	400	Performance Psychology and Strategic Resilience. Mosaic
Claudiu Andrei CERCHIA	420	The Blue Bastion: The Danube as a Resilience Line – Preliminary Considerations in National Defence Architecture
Romeo BOȘNEAGU	428	Arctic Navigation Routes: Past, Present and Future – Strategic, Geopolitical and Naval Implications of the Northwest Passage and the Northern Sea Route
Iulian DINULESCU	446	Emerging Forms of Religiously-Motivated Far-Right Extremism in Europe and North America: Risks and Projections for the 2025-2030 Period
DEFENCE RESOURCES MANAGEMENT		
Dumitru IANCU Anca DINICU	472	The Defence Resources Management in the Framework of the New European Security Objectives
Gabriel MĂNESCU Sebastian Emanuel STAN	486	The Impact of Artificial Intelligence on Specific Defence Resources Management Processes
Alexandru HERCIU Ionela Cătălina MANOLACHE	502	The Necessity of Implementing the Concept of <i>"Military Mobility"</i> at the National Level for the Deployment of Forces Participating in Operations by Land
Maria CONSTANTINESCU	520	Advancing the Strategic Resilience of Military Mobility Through a Whole-of-Government Approach

Dorel BADEA Diana Elena RANF Elisabeta-Emilia HALMAGHI	534	Educational Bootcamp for the Vocational Development of Adolescents in Resilient Societies – A Proposal Based On Project Management
Raluca RUSU	546	Resilience Among Future Military Leaders – Comparative Study Among the Students of the “Nicolae Bălcescu” Land Forces Academy
Daniel-Dorin CUCURĂ	556	Public Goods and Public Policies in the Field of Security: The Intersection between Economy and Defence Strategy in the Context of Contemporary Transformations
Iulian-Radu MONORANU	582	Approaches to the Requirements and Opportunities for Integrating the Romanian Armed Forces’ Key Capabilities in Allied Multi-Domain Operations
Vlad Ionuț DUMITRACHE	600	Using the ReARM Europe Program to Finance European States – Case Study: The Use of the Safe Instrument in Romania
George-Adrian AIONESEI Cristian DRAGOMIR	612	Shaping Modern Aviators: from Technical Mastery to Ethical Leadership
Ioan MUNTEANU Florin Ioan CIOANCA	628	Optimizing an Integrated Maintenance System for Vehicles
MILITARY HISTORY		
George-Daniel UNGUREANU	646	The Romanian Diplomatic Initiative of the “ <i>Neutral Bloc</i> ” in the Political-Military Context of the Black Sea (September-December 1939)
Dan-Dragoș SICHIGEA	672	The Last Stage of the Crimean Evacuation: Frictions between the Army and the Navy
Gavril Vasile BĂBAN	686	Radiography of Military Units from Baia Mare Garrison from 1990 to 2005
Ioan-Dan POPOVICIU	696	The Soviet Infantry Man on the Prut River: 22 June 1941 – Historiographical Perspective on Combat Training
Marian TĂNASE	704	Romanian-American Relations in the Naval Field (1975-1980)

FOREWORD

Colonel Cristian-Mihai CHIOREAN

The international environment of today is more and more defined by volatility, uncertainty, and the rapid acceleration of geopolitical, economic, and technological change. Within this context, the capacity of states to absorb shocks and to restore essential functions in a timely manner – commonly referred to as strategic resilience – has become a fundamental pillar of national defence. Strategic resilience encompasses the ability of national systems to anticipate, resist to and recover from a wide range of shocks and disruptions, including political crises, armed conflicts, cyber incidents, and natural disasters. Beyond immediate crisis response, it implies adaptability and the preservation of critical functionality under conditions of persistent uncertainty and changes. As such, strengthening strategic resilience has become a central objective of defence and security policies, directly contributing to state stability, sovereignty, and continuity in the face of the new global challenges.

Hybrid threats, ranging from information manipulation to disinformation campaigns, cyber operations, infiltrations, economic coercion, and the exploitation of critical technologies require advanced mechanisms of anticipation, prevention, and coordinated response. In this regard, structured dialogue among experts, military professionals, analysts, and political decision-makers plays a strategic role, fostering a shared understanding of evolving risks and supporting the development of coherent and effective solutions for the protection of national interests.

This volume brings together the contributions presented at **the seventh edition of the Romanian Military Thinking Conference, held under the theme “Strategic Resilience and National Defence: From Planning to Action in the Face of Hybrid Threats”**. Conceived as a platform for integrated debate, the conference facilitated both academic, scientific research and applied perspectives relevant to experts and practitioners in the fields of security, defence, and public policy. Through its thematic panels – **Theory and Military Art, Intelligence and Security, Defence Resource Management and Military History** – the event promoted a multidisciplinary approach to contemporary security issues, linking doctrinal analysis with operational insights and strategic assessment.

The conference was held at a time of increasing pressure on deterrence and defence systems, when the effectiveness of institutional responses to crises has become a key indicator of national resilience. Participants examined the evolution of NATO's deterrence and defence posture, emphasising the way it adapted to the changing international security environment. During the discussions, particular attention was given to the implications of disruptive technologies for the future of conflict, including artificial intelligence, autonomous systems, and the expanding role of cyber capabilities. The discussions also highlighted the importance of a realistic and forward-looking assessment of strategic risks in the Black Sea region, acknowledging both the complexity of this geostrategic space and the need for continuous adaptation in response to rapid technological and geopolitical developments.

Additional debates addressed the role of intelligence, influence activities, and cyber defence in contemporary military competition, as well as the contribution of civic resilience, innovation, and industrial cooperation to armed forces transformation. Emphasis was placed on doctrinal adaptation, organisational culture, and the development of multi-domain operations, which are increasingly central to the architecture of future defence.

Hybrid threats underscore the necessity of response strategies that are both precise and tailored to the heightened complexity of the current international environment. These challenges extend beyond the traditional boundaries of the military domain or the national defence, involving diverse actors and instruments, from disinformation, cyber attacks to economic pressure and indirect political influence. The conference provided a comprehensive framework for addressing these issues from a multidisciplinary perspective, encouraging the identification of pragmatic solutions that bear in mind both resource constraints and the complex realities of the current geopolitical and strategic-economic context.

The contributions included in this volume reflect the diversity of perspectives and the depth of expertise of the participants – researchers, military officers, security professionals, representatives of public institutions and international organisations. Through their analytical rigor and policy-relevant recommendations, these works aim to serve not only as a platform for intellectual convergence, but also as a reference point for future initiatives, policy development, and research agendas.

We extend our appreciation to all those who contributed to the success of the conference and to the realisation of this volume! It is our hope that the ideas, analyses, and conclusions presented here will represent a valuable resource for the defence community and for all stakeholders engaged in strengthening state resilience in the face of hybrid threats. We are confident that this collective effort will continue to stimulate dialogue, cooperation, and innovative solutions!

INNOVATIVE APPROACHES IN MILITARY LEADERSHIP AT STRATEGIC AND OPERATIONAL LEVEL – DECISIVE FACTOR FOR THE SUCCESS OF MILITARY ACTIONS –

Brigadier General Ștefan-Claudiu TOPOR

282nd Armoured Brigade “Unirea Principatelor”, Focșani

DOI: 10.55535/RMT.2025.3.01

The evolution of the global security environment, marked by uncertainty and complexity, requires a comprehensive approach of military leadership at the strategic and operational levels. This research paper analyses innovative approaches in military leadership, focusing on adaptability, the integration of emerging technologies and the development of cognitive and emotional skills of leaders. There are arguments brought to your attention that the success of military actions is not determined exclusively by technological or numerical superiority, a decisive role being played by the ability of leaders to anticipate and manage change, to make effective decisions under conditions of ambiguity and to coordinate multinational and inter-institutional structures. The decisive role of innovative leadership is highlighted in increasing organizational resilience and in achieving strategic and operational objectives in the contemporary security environment.

Keywords: military leadership; innovative approaches; global security environment; adaptability; organizational resilience;

INTRODUCTION

Military leadership has always played a decisive role in the success of military operations. History shows that victory did not always belong to the largest or most technologically advanced armies, but to those led by leaders capable of combining strategic vision, adaptability and discipline. Alexander the Great, for example, managed to conquer vast territories thanks to his ability to combine mobility and logistics with a coherent strategy and an overall vision of the situation. Hannibal remained in history through his operational ingenuity, using terrain and surprise to compensate for numerical inferiority. Napoleon revolutionized the organization of the army and the art of manoeuvre, but he also demonstrated the limits of a leadership that was too focused on his own will, the defeat in Russia being the classic example of the lack of sustainable logistics.

The 20th century brought dramatic lessons regarding the role of military leadership. In the Second World War, the Allies' ability to plan and logistically support a global campaign was decisive. Leaders like Eisenhower and Montgomery showed that success does not only lie in personal talent, but also in the art of coordinating coalitions and integrating resources. In the Cold War, strategists like Henry Kissinger and Lawrence Freedman emphasized the role of innovative strategic thinking in maintaining global balance.

Today, military leadership faces a much more complex reality. The concept of VUCA (volatility, uncertainty, complexity, ambiguity) faithfully describes the current strategic environment. Hybrid warfare, information warfare, the proliferation of non-state actors and the emergence of new technologies (artificial intelligence, drones, cyberattacks, space warfare) force leaders to adopt innovative leadership models. Rigid hierarchical structures, specific to the industrial age, are insufficient. The modern commander must combine doctrinal rigour with flexibility and creativity.

This article aims to examine how innovative leadership – at the strategic and operational levels – is a determining factor in military effectiveness. In this regard, the comparative analysis method is used to assess the impact of different leadership models on military outcomes. The analysis begins with classical doctrinal foundations (Clausewitz, Sun Tzu, Jomini, Liddell Hart, Huntington), continues with modern leadership models (transformative and adaptive) and integrates general conclusions from historical and contemporary conflicts: Second World War, Desert Storm, Kosovo, Iraq, Afghanistan and Ukraine.

DOCTRINAL FOUNDATIONS OF MILITARY LEADERSHIP

Carl von Clausewitz introduced fundamental concepts for understanding war, such as “friction” and “fog of war”. By friction, Clausewitz meant the set of unforeseen obstacles that inevitably arise in the conduct of military operations: adverse weather, technical malfunctions, human errors, incomplete information. The “fog of war” refers to the structural uncertainty that affects any commander. In this context, the effective military leader is the one who possesses that “*coup d’œil*” – the strategic intuition that allows him to decide correctly in conditions of ambiguity.

The relevance of these concepts is still seen today. In Iraq and Afghanistan, friction took the form of asymmetric attacks, coordination problems between allies, and errors of cultural perception. In Ukraine, the fog of war is amplified by information warfare and the use of drones for reconnaissance and strike, which constantly change the operational picture.

Sun Tzu, in *The Art of War*, proposed a different vision: the perfect victory is the one achieved without fighting. Strategy means deception, adaptability and the use of the opponent’s weaknesses. The military leader must be able to analyse the confrontation environment and act accordingly, using the principle of economy of forces, thus avoiding the unnecessary consumption of resources.

In asymmetric conflicts, Sun Tzu’s principles are clearly relevant. Non-state actors, lacking conventional force, compensate through mobility, surprise and exploitation of the effects of psychological and information operations. Contemporary military leaders must learn to think not only in terms of frontal confrontation, but also in terms of perception and influence.

Antoine-Henri Jomini tried to transform the art of war into an exact science. He emphasized lines of operations and the concentration of forces at decisive points. His contribution was major for the development of staff work and planned thinking. However, this type of rigidity has been criticized: the manoeuvre wars of the 20th century showed that mathematical geometry cannot capture the unpredictability of the human factor and the environment.

B.H. Liddell Hart proposed “*indirect strategy*” as an alternative to direct confrontation. He emphasized that great victories are achieved through surprise, manoeuvre, and striking the adversary’s centres of gravity where he least expects it. Indirect strategy inspired both the Normandy campaign of 1944 and Operation *Desert Storm* of 1991, where coalition forces avoided a prolonged frontal confrontation by using manoeuvre and technological superiority to defeat the Iraqi armed forces.

Samuel Huntington introduced an essential dimension: the relationship between military leadership and civilian control. In his vision, the military must

remain subordinate to political authority, but must have professional autonomy to accomplish its mission. For multinational alliances such as NATO, this vision is crucial: military commanders must harmonize political directives with operational realities, avoiding both blind obedience and excessive independence.

Strategic leadership is not just military planning; it is the act of coherently integrating all instruments of national power and international alliances into a vision capable of responding to emerging threats. In the modern era, this integration must include military, political, economic, diplomatic, and informational dimensions.

ADAPTABILITY OF LEADERSHIP AT THE STRATEGIC AND OPERATIONAL LEVELS TO THE REALITIES OF CONTEMPORARY CONFLICT

The modern strategic leader should be oriented towards the ability to anticipate changes in the global environment, the ability to formulate flexible visions and the power to mobilize the necessary resources. Without these traits, even the largest armed forces can become prisoners of their own inertia.

John Boyd, a Colonel in the US military aviation, formulated the OODA (Observe–Orient–Decide–Act) cycle, explaining that success belongs to the one who can process information faster, decide more correctly and act faster than the opponent. At the strategic level, this means that the leader must not only react, but also constantly create new situations, forcing the opponent to adapt.

The 2003 invasion of Iraq provided an example of the limits of insufficiently adapted strategic leadership. The initial military campaign was a rapid success due to technological superiority and the ability to project power. However, the lack of an innovative strategy for post-conflict stabilization created a power vacuum that was exploited by local and regional actors. Strategic leadership failed to anticipate social and political complexity, and the consequence was a protracted insurgency that undermined initial gains.

In Afghanistan, NATO forces demonstrated remarkable operational capacity, but strategic leadership failed to provide a coherent, long-term vision for state reconstruction. Insufficient integration of political, cultural, and economic factors reduced the effectiveness of military campaigns. Experience has shown that innovative strategic leadership is not just about winning battles, but also about creating the conditions for lasting peace.

Faced with these lessons, NATO developed the concept of a “*comprehensive approach*” – integrating military and civilian, national, and international efforts into a single, coherent strategy. It involves cooperation between military, governmental, and nongovernmental actors to address the complexity of contemporary conflicts. Innovative strategic leadership, in this context, involves not only military command, but also diplomacy, resource management and strategic communication.

Thus, it can be said that strategic success does not depend exclusively on the number of troops or technological performance, but on the ability of leaders to orchestrate all the instruments of power into a coherent and adaptable ensemble.

If strategic leadership sets the direction and objectives, operational-level leadership ensures their transposition into concrete campaigns and operations. It is the level where strategic intent meets the reality of the field.

Originating from the Prussian military tradition, the concept of *Auftragstaktik* – known today as *Mission Command* – requires the senior leader to establish the intent and objective, but to leave subordinates the freedom to decide how to execute the mission. This decentralization of decision-making increases agility and allows rapid adaptation to changing battlefield conditions.

In modern conflicts, where communication can be disrupted and situations change from one minute to the next, mission command becomes essential. The operational leader creates the framework and organizational culture that allow for initiative without losing the coherence of the whole.

The war in Ukraine provides an eloquent contemporary example. Ukrainian forces, although numerically and technologically inferior, have capitalized on tactical initiative and operational flexibility. Small units have used commercial drones, real-time information, and decentralized manoeuvres to create disproportionate effects. This is the practical expression of innovative operational leadership, able to compensate for material deficiencies through creativity and adaptability.

In contrast, the adversary has demonstrated structural rigidity, maintaining centralized chains of command and reacting slowly to changes in the situation. The result has been a loss of initiative and vulnerability to smaller, more agile forces.

Operation *Allied Force* in Kosovo has shown how leadership can turn political limitations into an advantage. Although constrained by the absence of UN approval and the desire to avoid civilian casualties, NATO managed to use air power in an innovative way to achieve political objectives.

Operation *Desert Storm* was also a demonstration of innovative leadership. Coalition commanders avoided a frontal confrontation, opting for a large-scale manoeuvre that disrupted the Iraqi armed forces and led to a quick victory. The main lesson: operational innovation maximizes benefits and minimizes costs when combined with rigorous planning and execution.

EMERGING TECHNOLOGIES AND THE LOGISTICS DIMENSION

In the 21st century, technology is no longer just a tool in support of war, but a central domain of confrontation. Artificial intelligence, drones, cyberwarfare, and the competition for supremacy in space are radically changing the balance of power.

Drones have transformed the battlefield, providing a real-time operational picture and precision strikes at low cost. Artificial intelligence promises an unprecedented acceleration of information processing and decision-making. Autonomous systems can act where the risk to humans is too great. However, these innovations raise ethical dilemmas and new risks: *Who is responsible for the decisions of algorithms? What happens if an autonomous system is manipulated or cyber-attacked?*

Modern leadership involves not only using new technologies, but also managing them responsibly. The commander must understand both the advantages and vulnerabilities and avoid excessive dependence on systems that can be compromised.

“Amateurs talk tactics, professionals talk logistics” – this expression, often attributed to General Omar Bradley, summarizes the reality of the battlefield. Liddell Hart considered logistics *“the lifeline of strategy”*.

In the Second World War, the US’s ability to project force across Europe and the Pacific was decisive. Operation *Overlord*, in Normandy in 1944, would not have been possible without extensive logistical preparation, including the construction of artificial harbours (Mulberry harbours). In Vietnam, the adversary’s logistics – the famous *“Ho Chi Minh Trail”* – allowed resistance against a much larger force. In Operation *Desert Storm*, the rapid transport of over 500,000 troops and millions of tons of equipment demonstrated that logistics can decide the speed and success of a campaign.

Today, the conflict in Ukraine confirms that logistics is decisive. Maintaining the flow of ammunition, equipment and fuel has become a test of national resilience and international alliance. Innovative leadership must treat logistics not as a technical detail, but as a top-tier strategic area, where creativity and anticipation are vital.

THE COGNITIVE AND INFORMATIONAL DIMENSION

In the information age, victory is not measured only in conquered territories, but also in the created perceptions. Qiao Liang and Wang Xiangsui anticipated, in *Unrestricted Warfare*, that the future war will include economic, informational and cultural domains, and that weapons will be not only guns but also ideas.

Joseph Nye introduced the concept of *soft power*, explaining that cultural influence and the ability to attract can be as effective as military or economic pressure. In modern warfare, these concepts converge: information warfare becomes a decisive environment of confrontation.

Disinformation campaigns, fake news, the use of deepfakes and manipulation of social networks have the potential to weaken social cohesion and undermine the will to resist. In Ukraine, information warfare has been almost as intense as kinetic warfare: both sides have tried to influence global perception and the morale of their own populations.

NATO has recognized this reality, creating centres of excellence in strategic communication and psychological operations. Innovative leadership involves integrating these tools, strengthening psychological resilience, and cultivating an organizational culture capable of withstanding information pressure. Thus, the commander is no longer just a manager of troops and resources, but also an architect of perceptions, a leader capable of winning the battle of narratives.

CONCLUSIONS

Sustainable military success depends on the coherent integration of the strategic, operational, and tactical levels. Ambitious strategies remain sterile if they cannot be translated into effective campaigns. Tactical victories become useless if they do not serve a clear operational and strategic objective. Modern innovative leadership is the glue between these levels. It ensures coherence and relevance, transforming local initiative into global effects and permanently adapting strategic objectives to the reality of the battlefield.

In conclusion, innovative military leadership is shaped as a synthesis between the classical foundations of strategic thinking and the adaptability requirements specific to the contemporary era. The theoretical legacy of authors such as Clausewitz, Sun Tzu, Jomini, Liddell Hart or Huntington continues to provide essential conceptual landmarks, but they can no longer be applied rigidly. Therefore they must be reinterpreted and integrated into a flexible framework, capable of responding to the challenges of an operational environment under constant change. Thus, tradition and innovation are not mutually exclusive, but complement each other, constituting the foundation of effective military leadership.

Also, innovation in military leadership is not reduced to the introduction of state-of-the-art technologies, but requires a much more complex approach. It means the ability to integrate multiple dimensions – logistical, informational, perceptual and cultural – into a coherent whole, which provides both operational mobility and strategic legitimacy. This holistic perspective allows the transformation of resources and information into sustainable competitive advantages on the battlefield.

The analysis of relevant case studies – the conflicts in Iraq, Afghanistan and Ukraine – clearly demonstrates that the lack of adaptive and innovative strategic and operational leadership can cancel out tactical gains. Victory achieved in specific confrontations risks being compromised when there is no coherent vision to ensure continuity and exploitation of the results. Thus, recent experiences show that military success is not measured only by the won battles, but by the ability to transform tactical advantages into long-term stability and security.

In conclusion, we can say that, in a strategic environment characterized by volatility, uncertainty, complexity and ambiguity (VUCA), innovative leadership becomes not just an option, but a doctrinal and professional obligation. Its absence can condemn military organizations to stagnation or failure, while its presence represents the guarantee of resilience and relevance in the face of emerging challenges. In this context, innovation in military leadership is not configured as a theoretical luxury, but as an indispensable condition for survival and operational efficiency.

BIBLIOGRAPHICAL REFERENCES:

1. Bass, B M. (1990). *From transactional to transformational leadership: Learning to share the vision. Organizational Dynamics*, <https://omsorgsforskning.brage.unit.no/omsorgsforskning-xmlui/bitstream/handle/11250/2656417/Bass.pdf?sequence=1>, retrieved on 12 September 2025.
2. Biddle, S. (2004). *Military power: Explaining victory and defeat in modern battle. Princeton University Press*, <https://core.ac.uk/download/pdf/36730773.pdf>, retrieved on 3 September 2025.
3. Boyd, J. (1987). *A discourse on winning and losing*, https://www.coljohnboyd.com/static/documents/2018-03__Boyd_John_R__edited_Hammond_Grant_T__A_Discourse_on_Winning_and_Losing.pdf, retrieved on 10 September 2025.
4. Burns, J.M. (1978). *Leadership*, <https://archive.org/details/leadership1978burn/mode/2up>, retrieved on 8 September 2025.
5. Clausewitz, C. (2006). *Despre război*. Editura Antet.
6. Freedman, L. (2013). *Strategia. O istorie completă*. Editura Litera.
7. Huntington, S.P. (1957). *The Soldier and the State. Harvard University Press*, <https://worldoriens.wordpress.com/wp-content/uploads/2017/03/the-soldier-and-the-state-huntington.pdf>, retrieved on 5 September 2025.
8. Jomini, A.H. de. (2008). *The Art of War*. Wilder Publications.
9. Kissinger, H. (1994). *Diplomacy*, <https://euroclassworks.com/wp-content/uploads/2015/03/download-kissingers-diplomacy.pdf>, retrieved on 14 September 2025.
10. Liddell-Hart, B.H. (1991). *Strategy*, <https://www.docdroid.net/KnjBIII/strategy-b-h-liddell-hart-pdf>, retrieved on 6 September 2025.
11. Mattis, J., Hoffman, F. (2005). *Future warfare: The rise of hybrid wars. Proceedings*, <https://milnewstbay.pbworks.com/f/MattisFourBlockWarUSNINov2005.pdf>, retrieved on 4 September 2025.
12. NATO. (2019). *Allied Joint Doctrine for the Conduct of Operations (AJP-3)*, https://www.coemed.org/files/stanags/01_AJP/AJP-3_EDC_V1_E_2490.pdf, retrieved on 14 September 2025.
13. Nye, J.S. (2004). *Soft power: The means to success in world politics*, https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/joe_nye_wielding_soft_power.pdf, retrieved on 12 September 2025.
14. Qiao, L., Wang, X. (1999). *Unrestricted Warfare*, <https://www.c4i.org/unrestricted.pdf>, retrieved on 15 September 2025.
15. Sun Tzu (2023). *Artă războiului*. Editura Cortex.

THE ARCHITECTURE OF COMMAND-AND-CONTROL SYSTEMS IN FUTURE MILITARY ACTIONS

Colonel Dr. Cezar POPA

Deputy Chief, 2nd Mountain Troops Brigade "Sarmizegetusa", Braşov

DOI: 10.55535/RMT.2025.3.02

Command-and-control systems are constantly adapting, resizing and developing in line with the technological evolution and the changes in the physiognomy of military operations. In this context, command-and-control systems become more complex and efficient, due to not only the quality of the military command personnel but also the systems architecture, which integrates and interconnects high-performance equipment. Moreover, the architecture of a complex command-and-control system is designed as a coherent integrator of sensors, decision-makers, executors and support capabilities, interconnected in subsystems to ensure the efficient planning, preparation, deployment and evaluation of military actions.

The main objective of the command-and-control systems is to obtain and maintain the informational decision and action superiority in the entire spectrum of military operations, which will guarantee the success at strategic, operational and tactical levels. Given the diversification of risks and threats in the multidimensional operational environment, the architecture of command-and-control systems must be permanently adapted in order to ensure real-time, horizontal and vertical communication between tactical level forces, operational and strategic command and support structures, as well as with the other institutions are also involved in the security and defence field.

Keywords: command-and-control systems; variable geometry; capabilities; technology; strategic, operational and tactical levels;

INTRODUCTION – STRUCTURES AND SYSTEMS OF COMMAND AND CONTROL

Military command-and-control systems, also known as C2 systems, are functional structures used by military structures to plan, conduct, assess and coordinate military operations.

In the past years, the way these systems are working has evolved in line with the changes in the conduct of military conflicts. The conflict with variable geometry, the most recent known type of conflict, has different forms, from “*peaceful revolution*”, “*civil war*”, “*war against terrorism*” and “*extended international conflict*”, involving multiple state and non-state actors (Revista Academiei de Științe ale Securității Naționale, 2019, p. 50). The Syrian conflict is the most recent example of a geopolitical and geo-economic conflict that started as a civil war (<http://www.contributors.ro/economie/energie-economie/razboiul-civil-din-siria-un-razboial-gazoductelor/>). The conflict was conducted on internal political level, with external foreign support, evolving to a conflict between super powers (the USA and the Russian Federation) in order to control the energy routes and resources. The conflict generated a huge humanitarian crisis, increasing migration and refugee flows towards neighbouring countries and the European Union. Some authors consider it as a “*4th generation conflict*”, at least one of the actors being a non-state entity (Impact strategic, 2017, pp. 56-57). This type of conflict generates multiple types of action – political, economic and military, that are conducted by combatants, insurgents, terrorist groups and civilians. This is an irregular and asymmetric conflict, using insurgent, guerrilla and terrorist TTPs against political, cultural, religious objectives or even against population.

Proxy war is another current concept. This is a conflict between two powers (armed forces, state actors) through interposed actors, on another state’s territory (Impact strategic, 2015, pp. 21-22). The parties do not directly engage each other, but interposed state and non-state actors are used.

In this context, we consider that expansion of command-and-control systems is necessary to manage both military operations and political-socio-economic-military operations specific to the new types of conflict. Command-and-control systems need to permanently adapt to new types of conflict and to the technological evolution.

All decision-makers need to be connected in real-time, both horizontally and vertically, facilitating the C2 of all conflict operations (at all levels – political, social, economic, military) based on an integrated situational picture. Both technology and an adequate C2 system facilitate a real-time response to dangers and threats.

There are three main trends in the evolution of C2 systems: technological developments, multinationalism and the expansion of operations in all areas.

Modern conflict environments are more complex, based on the evolution of technology and information. Non-military operations, diplomatic, political and economic actions have a certain position in the variable geometry of the conflict, but they are accompanied by complex, coordinated, planned military operations, more often than not at strategic level.

A C2 system vulnerabilities occur from within, while threats and risks are external.

Actions specific to modern conflicts represent a proof of the multidimensionality that generates a permanent shifting geometry along multiple axes (as a graphical representation of a conflict).

To each dimension of the conflict is corresponding a series of non-military operations like political-diplomatic ones (negotiation, inquiry, good practices, conciliation, arbitration, international judicial institution's decisions; UN Charter, Ch. 6), and economic (SMART sanctions – blocking personnel and institution assets, economic sanctions, embargo, blockade), as well as non-military actions (ethnic separatism, boycott, media attack) or military conventional operations (offensive, defensive, intermediate, stability, peace keeping, peace support and peace enforcement), unconventional operations (special ops, NBC), asymmetric operations (insurgent, organised crime, social unrest, revolution, civil war, guerrilla war, terrorism) and other types of operations (cyber, information, psychological, CIMIC).

Conflict's dimensions are evidence of operations conducted in all environments: physical (ground, air, maritime, space), cyberspace, information, giving to modern conflict its multidimensional character.

Command-and-control systems need to become a complex architecture entity, capable of managing full spectrum of operations, simultaneously, in all environments and dimensions.

Besides its interconnected elements (C2 structures, intelligence, communications and computer subsystems), command-and-control systems should include a variety of information management activities, procedures, equipment and other means used by commanders.

Conflicts with variable geometry require a modular C2 system with command, control, communications, computer, cooperation, intelligence, interoperability, surveillance and reconnaissance/C5I2SR (Lehaci, 2015, p. 65).

Therefore, it comes the requirements for new, unique infrastructure solutions, multiple multinational headquarters interconnectivity, adaptable and deployable modular C2 systems, sensors and base permanent monitor assets, based on modern technologies (identification, location and navigation) with discover, surveillance and target acquisition capabilities.

We consider that new services and new information may arise as a result of interconnection and/or integration of existing systems, included the use of artificial intelligence, with higher value and capabilities.

POSSIBLE ARCHITECTURE OF COMMAND-AND-CONTROL SYSTEMS IN CASE OF CONFLICTS WITH VARIABLE GEOMETRY

The roles, missions, objectives and C2 principles, the structural and functional interconnectivity/symbiosis of the system decision and operational command systems lead to an architectural C2 system according to the characteristics required to achieve the correct and efficient management of fluid/changing situations, specific to the conflicts with variable geometry (modular command-and-control systems as sum of systems and capabilities). The study of existing C2 systems, their evolution and trends represent an initial mark for a continuous structural development project, with the capability to rapidly adapt to any type of conflict or conflict combination. This undertaking is based on the permanent technological development and evolution.

The command-and-control concept has been continuously developed. In the first empirical approach, the concept evolved from C2 (command and control) to C3 (command, control and communications) then to C4 (command, control, communications and computers), to C4I (intelligence being added to this concept), eventually reaching to C4ISTAR (command, control, communications computers, intelligence, surveillance and target acquisition). The C5ISR modular system of systems adds interoperability and cooperation. The two systems that have been most recently added (interoperability and cooperation) are absolutely required in conflicts with variable geometry that integrate and overlap all other known types of conflict, with multinational, state and non-state actors and different domains as economic, social, political, military etc. Therefore, the structure of the system of systems will permanently change by adding components, or by combining them

in a way that may generate another superior subsystem compared to those that generated it, based on the operational reality of a conflict with variable geometry. In our vision, this modular system of systems will change according to its needs, using its subsystems, and it can create in short time another structure fit to respond the next operational challenge. We would compare this modular system of systems to a Rubik cube. Using the same components, the Rubik cube can display multiple solutions by shifting its parts. Likewise, command-and-control systems will rapidly change their structure, using the same modules and generating the adaptability and capabilities required by the new challenge.

The technological evolution facilitates new C2 systems, superior to those previously mentioned. For example, Network Enabled Capability (NEC) is the NATO concept for a system of systems used for an enhanced military effect in an integrated use of computer systems, based on the *“right information, at the right time, at the right place – not in excess”* (Mihăescu, 2016, p. 23) principle. This system has been built integrating decision-makers, instruments and support capabilities in order to conduct more flexible and more efficient military operations.

The advanced C2 system (AC2S), developed by the Defence University in the Czech Republic in 2017, represent a concept using modern technologies in order to enhance military operations efficiency. This system uses relatively new system architecture, communications, computer and decision support. Tactical decision support system (TDSS) is used as part of AC2S. The purpose of this system is to support the commanders in their tactical decision process by using generated models. AC2S develops the concepts of computer support in the decision processes. The researches in the data analysis using AI based on a technological support allow increased command and control efficiency.

Decision support systems (DSS) represent a tool for commanders used for information/intelligence exchange, information analysis, a tool that can help in an efficient mission planning process. An advanced DSS is capable of giving options to a commander in order to assess the chances of success, options to warn him on possible threats (Farlík, Kratký, Časar, 2016, pp. 327-330).

The general architecture of the AC2S is composed of three types of elements, as follows: the command point, the armed forces and robotic devices (systems), each with their role and missions. The command point is a main control centre with the following functions: situation assessment, operation planning and control, data collection and processing and analysis of available information, and dissemination through appropriate technical elements/equipment, command and control of forces, unmanned vehicles and robotic devices, communication with the upper

echelons. The forces are equipped with the tactical decision support system (TDSS). Unmanned vehicles and robotic devices can be included as long as they are compatible with the architecture (unmanned aerial vehicles/UAVs, unmanned ground vehicles/ UGGs, autonomous surface or underwater vehicles/AUVs). As for the high- precision hitting systems, they are connected through a wireless network so that they can benefit from the information and data from the command points.

AC2S's most important characteristic is that the system is modular. It can be configured for any type of military or non-military action/operation. Any available type or number of vehicles/assets can be included. Moreover, the militaries' number, together with their equipment for the following action/operation can be established according to the real requirements. The connecting wireless technology is compatible to all the elements. It comprises two independent networks, a short-range primary communication channel/network (messages, voice, images or video) and a long-range secondary channel/network (up to several kilometres), for back-up. The secondary channel/network is used when the primary network is no longer available. They are divided in underlets and interconnected elements. Even so, they can transmit only state information and control messages. That is why the system's capabilities must be enhanced.

The support of the decision-makers system (a subsystem of AC2S) is capable to understand the plan if there is an adequate model of tactics applied. The system is able to create optimal variants for problem solving by analysing the situation, the conditions and the effects. The courses of action are displayed for the commander in order to decide what solution to choose or the way in which to combine the courses. The subordinates and the robotic devices perform the decision. Each element knows its role and precise activity and tasks.

TDDS has the following capabilities: to prepare and to visualize the 2D geographical data, the operational areas' real time vectors and roasters, a real aid for several coordinate systems (geographical, WGS84/UTM, MGRS); it provides a basic geographical analysis (e.g. the topographical objects' analysis, direct and all round calculus visibility) (Rybanský, 2015, pp. 7049-7058) and also incorporates more advanced models of military tactics (5 advanced models of military tactics: the optimal manoeuvre for the units inside the area of operation, optimal model for monitoring systems' implementing, units' optimal logistic model, UAV optimal reconnaissance model and optimal land reconnaissance system).

More information about the TDDS can be found in *"Tactical Decision Support System to Aid Commanders in their Decision-Making"*, Modelling and Simulation for Autonomous Systems (Stodola, Mazal, 2016, pp. 396-406).

We have presented above a tactical model of a complex modular command-and-control system's architecture. However, when dealing with the threats and risks brought by a conflict with variable geometry, real-time communication, horizontally or vertically, between the national or multinational forces, command and support structures, as well as with the elements of strategic management or other elements with responsibilities in the field of security and defence is a decisive condition in obtaining the desired effects by executing the non-military or military operations. Tactical level modular systems must be operationally and strategically expanded so as to obtain the capabilities needed to effectively manage the challenges of extended conflict.

The news confirms that the technologies so far developed provide information flows in several areas like: the forces command and control, the common operational picture and common operational understanding, intelligence, surveillance, reconnaissance, strategic, operational and tactical planning, aerial situation and missile defence, joint fire, and air, naval and land target management, effects management, manoeuvre and synchronization, information operations, force protection, resource coordination, medical assistance etc.

The command-and-control system that is needed at the level of conflict with variable geometry must extend the interoperability, macro-surveillance and reconnaissance part at least at regional level, if not globally or extra terrestrially, in all conflict manifestation environments.

It is the moment when it becomes necessary to develop the artificial intelligence of cyber systems of systems based on integrated approaches of all the conflicting experiences developed over time that may generate, in advance, combined evolutionary conflict schemes in order to be managed before the real situation degenerate.

However, the context of technological development does not exclude the human element. It remains the most important element within the decision-making process supported by an adequate command-and-control system. Moreover, through the personnel who serves these technologies with their capabilities, the information becomes available to the decision-makers.

Comprehensive approach (CA) is the term that defines the need for joint effort to achieve governmental and nongovernmental goals when dealing with a conflict. To achieve this goal, simultaneous and convergent action is required on several directions of action: military, political (diplomatic), economic and civil.

Planning in order to achieve the common goal involves the information exchange, similar working methods and availability for joint planning sessions, which are more often than not carried out with difficulty. Planning in a multidimensional

environment and in the conditions of risks and threats specific to the conflict with variable geometry generates specific challenges for both civil and military actors. In open conflict situations, where the area of operations is assigned to a military commander, as well as due to the ability of the military system to plan actions of numerous forces, it is recommended that it should act as an integrator of the plans.

After completing the planning stage, the execution stage follows and automatically the implementation of the control measures of the operations/actions. The success of the actions depends on the execution of synchronized, joint and coordinated actions, and the command-and-control system, interoperable or common, of the allied forces must meet this condition. Under these circumstances, some institutions might not be willing to formalize relationships and exchange information freely.

The global security environment creates challenges that are so wide, so complex, volatile and difficult to anticipate.

CRITERIA USED FOR THE OPERATION OF MODULAR AND FLEXIBLE COMMAND-AND-CONTROL SYSTEMS

The integrated systemic approaches in the art of operational planning capture aspects related to the fact that the technologies developed to date provide information flows in several areas such as: command, control of the forces, common operational picture and its interpretation, intelligence, surveillance, reconnaissance, strategic, operational and tactical planning, air situation and missile defence, joint fire, and air, naval and land target management, effects' management, manoeuvre and synchronization, information operations, force protection, resource coordination, medical assistance etc. (Roman, 2017).

Starting from the premise that the command-and-control system adaptable to the requirements of the conflict with variable geometry must extend the interoperability part, macro-surveillance and reconnaissance at least at a regional if not even global or extra terrestrial level, in all the conflict environments, we consider that the development of artificial intelligence of cyber systems of systems becomes mandatory, based on the integrated approaches of all the conflicting experiences developed over time, which can generate early evolutionary combined conflict schemes in order to be managed before the degeneration of real situations.

However, the context of technological development does not exclude the human element. It remains the most important in the decision-making process supported by an adequate command-and-control system. Moreover, through the personnel who serves these technologies with their capabilities, the information becomes available for the decision-makers.

In this context, it is necessary to identify the precise conditions in which the dynamics of the contemporary operational environment takes place (by studying the multidimensionality of the current operational environment), to identify the typology of the specific threats of the conflict with variable geometry, to study in depth the organization of the headquarters (with the C2 systems and the necessary technological support for them to function) in order to draw relevant conclusions regarding their ability to respond to the requirements of conflict with variable geometry.

Starting from the existing structures and analysing the requirements that a command-and-control system must meet in relation to the challenges of conflict with variable geometry, other architectures based on modular structures with higher efficiency and multiple capabilities in different areas of conflict manifestation are outlined. Equipment and technologies play an extremely important part in this equation. They, in addition to the missions they have now, will have to provide the technical support in order to ensure the modules' mobility, subsystems and systems within the command-and-control system and the cooperation and interoperability with other systems of the same type. In this direction, the equipment used is based on the latest technological discoveries and developments. We have previously exemplified by Network Enabled Capability (NEC) a term used at NATO level for systems of systems designed to achieve increased military effect through an integrated use of information systems. But things will not stop there. The concept of artificial intelligence is being increasingly used. Extremely complex computer systems are capable of learning by themselves from the situations that are managed with their help. The researches in this field have developed artificial intelligence on the principle of the human brain's functioning. They can algorithmically and synthetically analyse and can also generate absolutely necessary quick solutions for the lack of time in the decision-making process. The commander may be offered in a relatively short amount of time certain courses of action already analysed through the necessary variables, already introduced within the system, and using a comprehensive database. The decision will be made much faster regardless of whether a system-generated or intuitive or combined course of action will be adopted. However, the human factor plays the most important role.

In the decision-making process, it is important *to integrate and interconnect the subsystems and technologies* necessary for the command-control operation. The identification and/or the construction of instruments for analysing the operational environment and the identification of the action procedures necessary for the command-control when managing specific situations of the conflict with variable geometry becomes imperative.

Any military conflict, no matter how insignificant it may seem, in any part of the world, will not be managed as an isolated fact, as a matter that concerns exclusively those directly involved. Each of these conflicts will increasingly require, for its resolution, a global solution, which triggers the involvement of the international community. Military conflicts and wars will be exposed because of sensors of any kind and not only. However, they will also be covert, in the space where the information can be used as a weapon. The entire cyber, psychological and information spectrum will be used to penetrate all networks in order to use them to gain a position that allows them to follow the desired courses. The new strategies and conceptions regarding the unfolding of current and future military conflicts are directly influenced by: the complex causality of the conflicts, which is due to the incompatibility between the dictatorial or autocratic and democratic political systems; the very large gaps that have been created over time between rich and poor countries; the effects created by the technological differences; the different ways of applying force, which go from the use of extreme violence (terrorist attacks) to the strategies of containment, domination or imposition of a certain type of behaviour; dissymmetry and asymmetry; predominance of alliance and coalition strategies; the mandatory existence of the binomial action-reaction; prevention and primitive or repressive character; responsibility.

Making anticipatory and correct decisions is conditioned by the military action's adaptation to the real strategic situations and the approach of all the conflict areas with variable geometry in planning and management.

The current multinational operations require the development and implementation of strategies, doctrines, forms of preparation and common staff procedures, as well as adequate programs for forces' equipping and planning. The responsiveness and increased interoperability will be possible through organizational flexibility.

Modularity will lead to an increased structural and actional mobility. The use of high-performance technologies will lead to a significant increase in the decision-making and action capacity regarding: increasing the distance of action and the precision that will enhance the selective and punctual engagement of some objectives; the ability to choose the target effect from a wide range of non-lethal and lethal effects, which will give the military decision greater flexibility; achieving the state of confusion necessary to obtain surprise and victory through psychological, information and error-induced warfare procedures; increasing the reaction capacity, optimizing the management and achieving the viability of the technical systems.

The result of using the high-performance technologies, *their integration and interconnection together with the subsystems* at C2 level will materialize in: significant increases in the systems and subsystems mobility as well as the decision-making capacity; increasing the anticipatory potential; broadening the range of planned and conducted operations; diversifying decision-making processes and procedures and conducting military or non-military actions/operations; new solutions for multidimensional forces/objectives protection.

CONCLUSIONS

Military command-and-control systems, known as C2, are functional structures through which military organizations plan, conduct, evaluate and coordinate military actions or operations. Conflict with variable geometry is the most recent known type of conflict that can start from a certain form (peaceful revolution or revolution) later escalating to forms of civil war, and/or war against terrorism and eventually embracing the form of extended international conflict.

The technological evolution facilitates the establishment of control systems such as modular control structures on command, control, communications, IT, cooperation, intelligence, interoperability, surveillance and reconnaissance (C5I2SR) and even more.

Taking into account all these aspects, the command-and-control system must become an entity with a complex architecture capable of managing all types of actions/operations carried out simultaneously, in all areas of conflict and in all dimensions.

In the conditions of conflicts with variable geometry, we are dealing with the existence of a modularized command-and-control system on structures, on command, control, communications, IT, cooperation, intelligence, interoperability, surveillance, reconnaissance etc.

In addition to the already outlined issues, there is the problem of developing unique infrastructure solutions, the possibility of interconnecting several operational headquarters belonging to actors from different states, command-and-control systems that have deployable command modules and that are adaptable to changing situations with implementation of sensor systems and permanent monitoring of the deployment of forces based on modern identification, localization and navigation technologies that are capable of ensuring the detection, surveillance and acquisition of targets and beyond. We consider that by integrating and/or interconnecting the already existing systems with new ones, we can obtain higher-value services and information, without excluding the possibility of the inclusive use of artificial intelligence.

The system must be able function as an integrator of decision-makers, sensors, executors and support capabilities, in order to obtain flexibility and efficiency in performing military and non-military actions/operations.

Under the risks and threats of a conflict with variable geometry, real-time, horizontal and vertical communication, between national or multinational forces, command and support structures, as well as with strategic management elements or other elements having security and defence responsibilities, we meet a mandatory condition with a decisive role in obtaining the desired effects by performing non-military or military operations.

In conclusion, we consider that the future architecture of command-and-control systems will be one of the system of systems-type and will include the human component, the information and virtual infrastructure, the modules for planning, managing and evaluating military operations, along with equipment based on artificial intelligence.

BIBLIOGRAPHY:

1. UN Charter, Ch. 6. *Peaceful settlement of disputes* and Ch. 7. *Action in case of threats against peace, breaches of peace and acts of aggression*, http://www.anr.gov.ro/docs/legislatie/internationala/Carta_Organizatiei_Natiunilor_Unite_ONU.pdf, retrieved on 12 August 2025.
2. Farlík, J., Kratký, M., Časar, J. (2016). *Detectability and jamming of small UAVs by commercially available low-cost means*. Bucureşti: IEEE International Conference on Communications.
3. Lehaçi, N.-T. (2015). *Tendințe în evoluția sistemului de comandă și control la nivel operativ*. Bucureşti: Editura Universității Naționale de Apărare "Carol I".
4. Mihăescu, C. (2016). Scientific research report no. 2, *Particularities regarding the evolution of command-and-control systems in future military operations*. Bucureşti.
5. *Revista Academiei de Științe ale Securității Naționale* (2019), no. 1, year IV.
6. *Impact strategic*, no. 3/2015, 1/2017. Bucureşti: Centrul de Studii Strategice de Apărare și Securitate/U.N.Ap.
7. Roman, D. (2017). *Abordări sistemice integrate în arta planificării operaționale*. Bucureşti: Editura Universității Naționale de Apărare "Carol I".
8. Rybanský, M. (2015). *Modelling of cross-country transport in raster format*, in *Environmental Earth Sciences*, vol. 74, no. 10, pp. 7049-7058.
9. Stodola, P., Mazal, J. (2016). MESAS 2016: Proceedings of the Third International Workshop on Modelling and Simulation for Autonomous Systems, *Tactical Decision Support System to Aid Commanders in Their Decision-Making*.
10. <http://www.contributors.ro/economie/energie-economie/razboiul-civil-din-siria-un-razboial-gazoductelor/>, retrieved on 19 August 2025.

DRONES – WEAPON SYSTEMS WITH A GROWING ROLE IN MILITARY CONFLICT –

Colonel (ret.) Dr. Romică CERNAT

*Visiting Professor, Department of Governance Sciences,
Faculty of Governance and Communication Sciences, Western University, Timisoara;
Member of the Romanian Reserve Officers Association*

DOI: 10.55535/RMT.2025.3.03

To strengthen national security, promote national interests, achieve or maintain technological superiority, and keep up with competitors, most states are increasingly focusing on developing effective and efficient military technologies. Drones are reshaping the way warfare is conducted in all domains. Recent conflicts, including the wars in Ukraine and in the Middle East, have been characterized by the use of drones on an unprecedented scale, making a relevant contribution to achieving success on the battlefield, which has triggered the race to develop cost-effective interceptors/drones against drones. The evolution of drones has gone, in a relatively short time, through several phases, moving from the target drone to the space-operating drone.

The lessons of war have generated questions regarding the possibility of replacing traditional weapons by drones, their classification as a type of weapon, as well as challenges regarding their reliability, potential advantages and disadvantages. Drones have proven effective in operations and environments where other types of technology are difficult to use. The primary motivation for drone using – getting soldiers out of harm's way – has been recognized during this period. Amid rising geopolitical tensions, technological advances in drones and artificial intelligence continue to reshape warfare and transform the battlefield.

Keywords: drones; unmanned aerial vehicles; reconnaissance; surveillance; swarming drones; UAV;

INTRODUCTION

The great powers have recently given increased importance to the development of emerging military technologies that have demonstrated, in recent conflicts, that they have a relevant contribution to consolidating and guaranteeing national security, in obtaining or maintaining supremacy in potential conflicts, as well as to keep up with other competitors. We are living in a world defined by conflicts that are seemingly difficult to resolve, heightened competition between great powers, and growing challenges generated by climate change, nuclear proliferation, and economic uncertainty (Miller, 2025, pp. 1-2).

Ever since the bow and arrow were invented thousands of years ago, killing from a distance, in one form or another, has been a defining feature of warfare. Drones have become essential to national security doctrines and strategies. They all essentially perform the same functions: providing intelligence, surveillance, and reconnaissance to wartime decision-makers and neutralizing adversary personnel and equipment. The US military's drone fleet ranges in size, shape, and sophistication, from the ground forces' hand-launched *Raven* drones to the Air Force's *Global Hawk*, which can reach altitudes of 20,000 m (Shaw, 2014, p. 1).

Emerging technologies and strategic competition between great powers mean that evolving technological advances, such as artificial intelligence, machine learning and anti-access/area denial capabilities, lethal autonomous weapon systems and, most recently, *drones* create difficult situations for military decision-makers in conducting combat actions but also in executing logistical support operations. Armed forces must be provided with equipment to execute precision strikes, at a distance, penetrate anti-access/area denial capabilities, and ensure efficient logistical support. To meet these challenges, there is now increased pressure to stimulate innovation, test new technologies, and implement them in the shortest possible time.

The emergence and development of *unmanned aerial vehicles (UAVs)*, commonly known as *drones* (*technology that has adapted to the new operational requirements and operates in all domains*), have revolutionized the way warfare is conducted, representing an evolution that influences the future of the national security of the great powers. Although, initially, the main purpose of drones was surveillance, reconnaissance and intelligence collection, they were later equipped

with weapons for use, in a new type of action or strategy carefully planned, to achieve a specific purpose, in counterinsurgency campaigns or in the so-called “*War on Terror*” as well as in military combat actions (Haqpan, 2013, pp. 1-5). Unmanned systems – drones – are fundamentally changing how forces of all sizes, as well as non-state actors achieve their objectives and how military equipment and capabilities are employed (DoD, 2024, pp. 1-2).

The war in Ukraine has been characterized by the deployment of drones on an unprecedented scale, thousands of drones have been used to track enemy forces, direct artillery fire, and strike targets. Analysing the effects of the use of drones, it can be concluded that they represent a technology that transforms warfare (Zafra, 2024, p. 1).

Drones represent *recent topics of interest* for: analysis, debate, lessons learned, security strategies and doctrines, future force structure; identifying and countering threats posed by: adversaries with similar military capabilities, “*rogue states*” and emerging technologies; and, the impact of major global risks. The world has entered an era of drone warfare. In five major interstate wars in recent years – those in Libya, Nagorno-Karabakh, Syria, Ukraine, and the Middle East – armed drones have played a dominant, perhaps decisive, role. There are debates about their use against non-state actors, or speculation about their potential role in war between the United States of America and close competitors such as China (Lyall, 2020, p. 1, 14).

Drone warfare is one of the most relevant developments in international security of the 21st century. Drone attacks have been used in various conflicts and by different actors, including the USA, Russia, Turkey, Azerbaijan, Ukraine, Iran, Israel, Nigeria, Iraq, Saudi Arabia, the United Arab Emirates and militant groups, reaching a record number of 805 Russian drones in a single night in September 2025 (Chiu, 2025, p. 7). The USA has carried out thousands of drone attacks, from attacks on non-state actors such as al-Qaeda to the January 2020 operation that killed Iranian General Qasem Soleimani. Turkey used armed drones domestically against the Kurdistan Workers’ Party and in Syria in 2020, marking the first time a country has used UCAVs (unmanned combat aerial vehicles) in a large-scale conventional attack on the battlefield (Horowitz, 2020, pp. 1-2).

In the war in Ukraine, which began on 24 February 2022 with the large-scale invasion of Ukraine by the Russian armed forces, *drones have become a fundamental technology* in the conduct of military actions. These cheap, unmanned flight systems, generally no heavier than a few kilograms and assembled from relatively simple, commercially available components, have sometimes caused significant destructive effects on the armed forces of both conflicting countries, especially Russia, but also

on civilians in Ukrainian localities. The importance of these technologies quickly became apparent to both Kiev and Moscow. Both have developed ambitious strategies to stimulate their domestic production of versatile aerial platforms and to support innovation in order to continuously overcome new countermeasures used by the enemy (Höller, 2025, pp. 1-3, 15-20).

Drones are used to provide useful imagery and information to make more effective and timely data-driven decisions. Artificial intelligence has the potential to produce a force multiplier effect by optimizing human capabilities and adding superior capabilities to less expensive military systems. For example, a single low-cost drone is harmless against a high-tech system like the *F-35 stealth fighter*, but a “*swarm*” of such drones could overwhelm high-tech systems, thus generating operational advantages and simplifications in the achievement of logistical support and, at the same time, transforming some current platforms into relatively outdated equipment. Technological advances are significantly influencing modern warfare – where robots, *swarming drones* and weapons using artificial intelligence could one day rule the land, the sky and the seas (Sayler, 2020, pp. 13, 29).

Drones are changing the way combat operations are conducted. This technology is gaining more and more attention and promises to bring a higher level of efficiency in tasks such as *data and image acquisition* of areas of interest, *location and tracking of specific targets* (target detection, classification and identification), *map compilation*, *communication relay operation*, *border patrol*, ***military operations***, *persistent surveillance of large areas* and *search and rescue*. Therefore, the use of such systems offers a credible alternative to manned aircraft. They operate in more dangerous conditions, with greater autonomy and can be very cost-effective compared to manned aircraft (STANAG 4586, 2014, p. 3-1). Recent conflicts also show how drone exports have increasingly become a *diplomatic tool* and with the increase in drone use, states have leveraged drone exports to increase their *global influence* (Greenberg, 2022, pp. 1-5).

In recent months, there has been a remarkable increase in the number of wars involving *nuclear powers*. Between 7 and 10 May 2025, India and Pakistan exchanged artillery fire, bombs, cruise missiles, and *drones* in the most intense round of fighting since 1999. Then, on 1 June 2025, Ukraine carried out a sophisticated covert operation – an unprecedented direct attack on a country’s nuclear deterrent, neutralizing bombers that Russia would use if it ever launched a nuclear attack. And on 13 June, 200 Israeli aircraft carried out a surprise attack on Iranian nuclear facilities and strategic targets (Malkasian, 2025, p. 1).

BRIEF HISTORY OF THE EVOLUTION OF DRONES. CLASSIFICATION

The records of drone use date back to the 19th century, when approximately 200 unmanned balloons containing bombs were used by the Austrians against the city of *Venice* in 1849. Later, similar balloons were used in the American Civil War in 1862 and the *Spanish–American War* in 1898 for reconnaissance and bombing purposes, producing some of the first aerial reconnaissance photographs. Aerial surveillance was used extensively in the First World War (Vyas, 2025, pp. 1–7; IWM, 2025, pp. 1–12).

Drones, like other land, air, sea and space platforms, are a form of *power projection*. They provide the ability to launch attacks without necessarily putting personnel in direct danger. It is rare to find a technology that can *change the nature of war*. In the first half of the last century, *tanks and aircrafts* dominated the way war was fought. The fifty years that followed were dominated by *nuclear warheads and intercontinental ballistic missiles*, weapons that shaped doctrines to prevent states from ever using them. The advent of *armed drones* overturned this calculation: *war was possible precisely because it seemed so risk-free*. The “bar” for the level of warfare had been lowered, the era of remote control had begun, and killer drones became last generation equipment (Shaw, 2014, p. 24).

Drones, either crudely constructed or improvised, have been used since the First World War, but reached a high level of sophistication in the Yugoslav wars of 1991–2001 and in the wars in the Middle East. The USA first used an armed drone in late 2001 in Afghanistan. 3 November 2025 marked 23 years since a remotely controlled drone was first used to commit extrajudicial killing “*beyond the battlefield*” to hunt down and kill individuals in a country with which the USA was not at war. Another example is the attack on a vehicle in Marib province, Yemen, target: Qa’id Salim Sinan al-Harithi (Dronewars, 2022, p. 1).

The main phases in the evolution of drones are described below. For each *phase*, the following *criteria* will be referenced: 1. *Time period*; 2. *Institutions*; 3. *Military logic/reasoning*; 4. *Key geographic areas*; 5. *Spatial logic/reasoning*; 6. *Iconic drones*.

Phase 1 – target drone: in the early 21st century, drones were used as training dummies. *Criteria description*: 1. Early 21st century; 2. Army, (USA); 3. Drones were used as practice dummies; 4. Developed at military shooting ranges in the UK and USA; 6. Hewitt-Sperry automatic airplane, Kettering torpedo.

Phase 2 – drone - flying bomb: in the interwar period and during the Second World War, the drone was imagined as a kind of flying bomb that could be launched behind enemy lines. *Criteria description*: 1. Interwar period; 2. Air Force,

USA; 3. Drones were used to deliver bombs and deliver messages to the enemy's disposition; guided to the target by radio; 4. Tested across the English Channel; 5. Cross the battlefield, bomb the enemy in depth; 6. Glide bomb, modified B17 bomber (Aphrodite, GB-Glider Bomb, 1943).

Phase 3 – surveillance platform drone: during the Cold War, it was used for gathering intelligence in restricted areas. *Criteria description:* 1. Cold War, Vietnam War (1964–1975), especially after the Cuban Missile Crisis; 2. Air Force and Strategic Command, USA; 3. Drones were used to photograph denied or dangerous areas; 4. Drones were used in North Vietnam, Cuba, China; 5. Battlefield surveillance, capture photos; 6. Various drones “Firebee”, “Bat”, “Ryan 147”, “AQM-34”, also known as Lighting bugs.

Phase 4 – the hunter-killer drone: since the outbreak of the war on terror (11 September 2001) the drone has been transformed into a *weapon*, combining *surveillance with killing*, thus becoming a combined hunter-killer or predator. *Criteria description:* 1. Post 11 September 2001; 2. US Air Force, CIA and JSOC; 3. Drones were used in a military “manhunt” during the war on terror; 4. Afghanistan (AF), Pakistan, Yemen and Somalia (CIA, JSOC); 5. Hunting dangerous individuals in the battle space; 6. Predator, and later the Reaper drone, as well as the Reaven portable drone.

Phase 5 – the drone as a police technology in domestic law enforcement. *Criteria description:* 1. Post 11 September 2001; 2. Police Forces, Customs and Border Patrol; 3. Drones are used by police forces in the USA and Europe; 4. Cities in the global north, used by hobbyists and criminals; 5. Monitor the street, protect VIP buildings; 6. Various drones (unmanned helicopter with four rotors).

Phase 6 – drones for intelligence collection, surveillance and reconnaissance combined with the ability to destroy personnel and equipment (Shaw, 2014, pp. 6-8) and *intercept drones* have been used in attacks in Pakistan, Ukraine, the Middle East (Ruitenbergh, 2025, pp. 1-6). Drones represent an increasingly greater challenge, confirmed by the War in Ukraine. These systems can track and hit moving tanks, artillery pieces and command posts or radio electronic means (Gosselin-Malo, 2025, pp. 1-6). Both sides involved in the Russo-Ukrainian war use drones, making it one of the first modern examples of drone use in an ongoing war (Gillis, 2024, pp. 1-10).

In response to the growing challenges posed by electronic warfare systems, both Ukraine and Russia are racing to develop next-generation drones guided by artificial intelligence. These drones identify and lock onto their targets without the need for communication with their operator, making them impervious

to signal jamming (Zafra, 2025, pp. 3-15). With Ukraine and Russia deploying millions of drones on the battlefield, the race to develop “*Octopus*” interceptors/drones – a “*new and advanced air defence interceptor drone*” – latest generation, *cost-effective* and *highly combat-effective* military equipment – began. *Criteria description*: 1. War on Terror, 2001, 2004-2015, War in Ukraine 2022-2025, War in the Middle East; 2. Land Forces, Special Forces (USA, Russia, Ukraine, UK); 3. Drones are used to neutralize personnel, equipment and infrastructure; 4. Pakistan, Ukraine, Middle East; 5. Detects and destroys personnel, armoured vehicles, and drones; 6. The MQ-1 Predator, Bayraktar TB2, Shahed 136, Ukrjet UJ-22, Orlan-10, Octopus.

Phase 7 – naval surveillance drones, which include both *surface and underwater vehicles*. In 1898 Nikola Tesla built the first radio-controlled ship, a boat (Ruitenbergh, 2025, pp. 1-6; Chiu, 2024, pp. 1-9) and Germany launched an underwater surveillance network with drones (Gosselin-Malo, 2025, pp. 1-3). The USA is pursuing an “*integrated three-dimensional surveillance system*” consisting of warships, submarines, aircraft, satellites, underwater drones, underwater microphones, and surface ships, and the Indo-Pacific region has become the main arena of military competition between the United States of America and China (Peck, 2025, pp. 1-6). In November 2016, the US Navy completed a test of a “*swarm*” of five unmanned boats equipped with artificial intelligence, which intercepted an “*intruder*” ship. The results of this experiment could lead to the adaptation of artificial intelligence technology for harbour defence and for other underwater missions, such as submarine hunting. *Criteria description*: 1. Starting with the Cold War Period, 1950, 2016, 2022-2025; 2. Naval Forces of China, USA, Russia, Germany; 3. Drones are used for underwater surveillance to detect enemy submarines and ships, destroy underwater sensors; 4. Indo-Pacific region, North Sea and Baltic, Greenland-Iceland-United Kingdom intersection; 5. Detects and classifies a variety of underwater threats; 6. SG-1 Fathom drones, Lura.

Phase 8 – space-operating drone (Sayler, 2025, p. 15). In the period 2021-2024 NASA used an autonomous drone that operated on Mars (Gillis, 2024, pp. 16-20). There are programs for the development of advanced aerospace attack capabilities based on reusable propellants (Kunertova, 2021, p. 69). Kinetic interceptors – drones – deployed in space do not have the constraints specific to other environments, but due to continuous movement, they cannot station or monitor an area for a long time, implying a *constellation* of such means to achieve permanent coverage of areas of interest (Karako, 2022, pp. 1-8; Shaw, 2018, pp. 1-8).

Criteria description: 1. 2021-2024, NASA used an autonomous drone operating on Mars. Interceptors – under study after 2022; 2. National Aeronautics and Space Administration/NASA; 3. Drones are used for endo-atmospheric interception of missiles, satellites. Aerospace attack capabilities based on reusable systems; 4. Space; 5. According to the data received from the sensors, it destroys missiles, satellites, sensors etc.; 6. Ingenuity Mars Helicopter. Equipment similar to the Falcon 9 rocket¹.

Classification of drone systems. The design, operation and regulations of aircraft vary greatly depending on their type and intended use. Aerial systems are classified in terms of the *existence of a crew* into two categories: a) *manned systems* and b) *other categories of aircraft*, which also include *unmanned aerial vehicles (UAVs)* or *drones*. Each category of aircraft has several subdivisions/classes. Aircraft are classified, certified and used in civil, general aviation, military (*developed for combat*) or other type of aviation asset (Abdullah, 2023, pp. 1-12). Drones can be classified, *according to the type of actions they support*, into two categories: those used for *reconnaissance and surveillance* purposes, in support of military actions and those armed with weapons for the purpose of *conducting military actions* (Boussios, 2015, pp. 1, 43).

Drones are *classified* according to different criteria: *wing type* (1. *with rotor* and 2. *with fixed wing*); *weight* (*very small* – 200 g, *small* – up to 1 kg, *medium* – up to 20 kg, *large* – weigh over 20 kg); *range* (*very small* – up to 5 km, *small* – up to 50 km, *short* – up to 150 km, *medium* – up to 640 km, *long* – over 640 km); *energy source* (battery, gasoline, hydrogen fuel cell and solar) and *type of activity* (toy, for photography or videography, racing, *FPV* drones (a “*first-person view*” drone – which transmits a live, real-time view from its camera to the operator, who sees it either through special glasses or on a monitor), search and rescue, *military*, construction and agricultural) (Gillis, 2024, pp. 1-10).

THE POTENTIAL FOR EMPLOYING DRONES IN ARMED CONFLICTS

Reconnaissance, surveillance, intelligence collection and fire assets neutralization are essential for maintaining information advantage, superiority in personnel and equipment on the battlefield and mission accomplishment, and unmanned aircraft,

¹ Sources for Criteria Description: Shaw, 2014, pp. 1, 6-8, 24; Gosselin-Malo, 2025, pp. 1-3; Gosselin-Malo, 2024, pp. 1-6; Peck, 2025, pp. 1-6; Brock, 2023, pp. 1-10; Gosselin-Malo, 2025, pp. 1-3; Gillis, 2024, pp. 1-10, 16-20; Zafra, 2024, pp. 1, 3-15; Kunertova, 2021, p. 55, 69; Becker, 2020, pp. 3-5; Franke, 2017, pp. 1, 3-12; Sayler, 2020, pp. 1, 13 -16, 29; Ruitenbergh, 2025, pp. 1-5; Chiu, 2025, pp. 1-9.

flexible and agile, help to provide extensive battlefield coverage, while being difficult to detect and intercept. This chapter will explore the role of drones in surveillance, battlefield reconnaissance, striking targets and achieving objectives, potential advantages, disadvantages and limitations of drone use and challenges in collecting and evaluating data and acting on timely reconnaissance data.

In the past year, unconventional warfare has undergone rapid changes, from cyber and information warfare to the use of drones (unmanned aerial vehicles) in all environments, air, land and sea, with an unprecedented development of drone and counter-drone technology in all theatres of operations, simultaneously generating debates about the features of the force of the future. We are witnessing a technological revolution, and new technologies, especially drones, due to their results on the battlefield, are being implemented at a rapid pace by all armed forces. Drones contribute to maintaining the efficiency of combat, support and logistics forces, to strengthening the resilience and capacity to support the reaction posture of the armed forces. They also contribute to preparing the force of the future, modernizing weapon systems and rethinking the entire defence ecosystem, from industrial production to force training (Ruitenbergh, 2025, pp. 2-5).

Characteristics of swarming drones – they have a *degree of autonomy* (not under centralized control), are able to detect their local environment and other participants, communicate locally with drones in the swarm and cooperate to accomplish a specific task. “*Swarming*” is a part of the development of autonomous vehicles, with uses ranging from large formations of “*low-cost*” drones designed to *overwhelm* defensive systems to small squadrons of drones that coordinate to provide *electronic attack*, *fire support*, and *localized navigation and communications networks* for ground troop formations (Sayler, 2020, pp. 14-15).

Integration of Drones into the Force Structure – Features, Characteristics

As militaries struggle to learn the lessons of the war between Russia and Ukraine, one question looms above all: *Can drones replace traditional weapons, such as aviation, tanks, and artillery?* Effective use of drones also requires developing the tactics, techniques, and procedures of the force categories that operate them, while integrating the use of drones into combat or combat support structures, reshaping operational requirements for military equipment, and accelerating military innovation cycles across all militaries (DoD, 2024, pp. 1-2). The military use of drones in the air, land and sea is booming, as well as the need to ensure their energy source. The war in Ukraine confirmed that batteries, and therefore essential

minerals, are truly important for both drones and communications. *Almost 80% of weapons systems rely on essential minerals* (Williams, 2025, pp. 1-3).

Chinese arms manufacturers are selling drones, promoted as capable of full autonomy, including the ability to carry out lethal targeted attacks. Some analysts warn that the proliferation of AI systems could decouple *military power* from population size and *economic power*. This decoupling could allow smaller countries and non-state actors to have a *disproportionately large impact* on the battlefield if they are able to take advantage of the scaling effects of AI (Sayler, 2020, pp. 16, 29).

An *unmanned aerial vehicle* (UAV) or *unmanned aircraft system* (UAS), often referred to as a drone, is an aircraft without a *physical human pilot on board*. Instead, a ground operator controls the flight of the UAV remotely via a communications link. Drones can be *remotely piloted* from a ground station or can *fly autonomously* using signals from ground-based sensors. The term *Unmanned Aerial System* (UAS) is often used in reference to drones because it emphasizes the importance of elements beyond the UAV, which generally include ground-based control systems and support equipment, such as a *command centre*.

The US Federal Aviation Administration (FAA) defines a UAV as a “*motorized aerial vehicle (powered by mechanical or electrical power) that does not have a human operator on board, uses aerodynamic forces to provide lift off the ground, can fly autonomously or be remotely piloted, can be disposable or recoverable, and can carry a lethal or non-lethal payload*”. It means that a UAV generally falls into the category of *powered take-off and landing aircraft*. Small UAVs/drones mainly use lithium-ion (Li-ion) or lithium-polymer (Li-Po) batteries to power electric motors. UAVs/drones are *powered by internal combustion engines or hybrid internal combustion engines and electrical sources* (a facility where electricity is generated for distribution). In the United States of America, the FAA defines any unmanned or *unoccupied aircraft* as a *drone*, regardless of its size or weight. Therefore, a *radio-controlled aircraft* is always officially classified as a *drone* if it has a flight control system that allows it to *fly autonomously (the human operator is part of the target selection and strike decision process)* (Embry-Riddle, 2022, pp. 1-26).

UAVs have most often been associated with the military, with drones being deployed on missions deemed too dangerous for manned aircraft. They were initially used for anti-aircraft training, intelligence collection and, more controversially, as *weapon platforms*. For military purposes, drones have two basic functions: flight and navigation. In order to fly, drones must have a power source, such as a battery or fuel. They also typically have rotors, propellers, or wings, and a frame.

Drones require a “controller”, which allows the operator to use remote controls to launch, navigate, and land the aircraft – all while the pilot remains on the ground. Controllers communicate with the drone using radio waves, such as Wi-Fi. Drones also typically have an onboard camera, which transmits what it sees to the operator’s control system. Some drones can automatically fly a set path using a *combination of sensors* to detect obstacles for collision avoidance and *GPS*. A common implementation of this function is the return-to-home feature on some consumer drones (Gillis, 2024, pp. 16–20). The British drone, the Zephyr, can fly non-stop for over 82 hours, is less expensive and does not involve exposure to risks for its own personnel (Boussios, 2015, p. 43). *The initial use of drones* was as weapons in the form of remotely piloted aerial missile *launchers*.

Drone features vary depending on the intended use. Examples of distinguishing attributes or aspects, features or inherent parts include the following: various types of high-performance cameras; artificial intelligence to have the ability to track targets; augmented reality features that overlay virtual objects on top of the drone’s camera feed; media storage format; maximum flight time, which determines how long the drone can stay in the air; maximum speeds, including climb and descent; hover accuracy (an aircraft that can hover in one place in the air); obstacle sensing range; altitude hold, to keep the drone at a fixed altitude; live video feed; flight logs; automatic return to home point and tracking mode (Vyas, 2025, pp. 1-25).

New drone strategies have already emerged, with US Secretary of Defense Pete Hegseth arguing in a July 2025 *Memorandum* that small drones should be *treated as munitions*, not aircraft, an aspect that could spur drone production and move forward very quickly. *The Memorandum* regulates several essential aspects. Most importantly, it treats small drones *under 25 kilograms* – so-called *Group 1 and 2 drones* – as *consumables* rather than “*durable goods*” (Tucker, 2025, pp. 1-10). In recent years, there have been debates in the USA about the rapid expansion of drone forces, the production of prototypes, experiments, and especially a doctrine regarding the use of drones in a war similar to the one in Ukraine.

One experiment in Indiana featured a pickup truck carrying a refrigerator-sized box in the middle of a field, from which six drones emerged in succession from a “hive”, rose into the air, and remained stationary to strike the target. Inside, screens showed the target, as well as the location of other elements, network connectivity, and more. The drones then moved to eliminate the target: an armoured vehicle some distance away. No actual large-scale coordinated fire materialized. But the most important elements of the demonstration were invisible: *a network of new*

detection, communication, and autonomy technologies working together under tight time constraints to show a new way forward for drone warfare – one with all the elements that the Ukrainians say they wish they had had in greater numbers from the start. They include *better communications, concrete doctrine, and a robust manufacturing base* (Tucker, 2025, pp. 1-10).

The USA is already working to develop ground force tactics, techniques, and procedures for operating FPV armed drones with operator vision while integrating the use of drones by infantry units. In May 2025, the USA announced that *the YFQ-44* combat aircraft, an *autonomous drone* designed to fly alongside the most advanced air force fighter jets, had officially begun ground testing. Advances in artificial intelligence and the use of drones in combat operations continue to argue that they represent an effective technique, leading the armed forces of many states to adapt their defence doctrines and strategies and to identify new companies that can provide them with the necessary drone stocks (Losey, 2025, pp. 1-15). Drone dominance is both a *process race* (a series of actions or steps taken to achieve a specific goal) and a *technology race*. Modern battlefield innovation requires a new procurement strategy that connects manufacturers with frontline troops. Fighting forces will take a technological leap, equipped with a variety of low-cost drones, manufactured by top engineers and artificial intelligence experts.

Leaders of major powers have pledged to rebuild militaries *to match threats with capabilities*. *Drones are the biggest battlefield innovation in a generation*, accounting for most of the casualties in the past year of the war in Ukraine. Global production of military drones has skyrocketed in the past three years. The realities of the modern battlefield have demonstrated that combat structures must be equipped with *small, lethal drones*. The US Department will invest in *unmanned aerial systems (UAS)*, such as single-strike capabilities and *loitering munitions*. By the end of 2026, each infantry group will have disposable, low-cost drones, with priority given to Indo-Pacific combat units and in accordance with other strategic guidance documents from the Secretary of Defense (Secretary of Defense, 2025, pp. 1-5).

The results of using drones in war. On 14 April 2022, Ukrainian forces stunned the world when they sank the heavily armed cruiser *Moskva*, the flagship of Russia's Black Sea Fleet, managing to hit the ship with their homegrown *Neptune* missiles, despite the ship's significant defences and the coordinated support of *Bayraktar TB2* unmanned drones, which are not detectable by radar (Cagaptay, 2022, p. 1). What seemed like a theoretical possibility became frighteningly close

to reality in June 2025, when Ukraine's *Operation "Spider's Web"* took place. Ukrainian agents spent months illegally smuggling hundreds of drones into Russia. In a coordinated attack, more than 100 small drones destroyed between 20 and 40 Russian warplanes at five air bases spread from Moscow to Siberia. The damage was a blow to Russian air power or the Kremlin's pride. Drone footage of burning bombers sent a terrifying message to nations around the world. If it could happen to Russia, it could happen to any country, including the United States of America. Operation Spider's Web represents an event, discovery, or change that marks a milestone or turning point in the use of drones. The emergence of small, easily transportable drones warns that even facilities thousands of kilometres from the contact line are not safe (Peck, 2025, p. 1). Beginning on 13 June 2025, as part of Operation Rising Lion, Israel used single-target attack drones that had been smuggled into Iran piece by piece to destroy Iranian air defences, helping Israel gain full control of Iranian airspace (Horowitz, 2025, p. 1).

The concentration of anti-aircraft systems near the front lines has created a no-fly zone for aviation and has amplified the role of drones, especially FPV drones, small and cheap drones that have become one of the most powerful weapons in the war in Ukraine. They take off from improvised platforms located from 5 km to 20 km from the front line, depending on the battery capacity and payload, are usually controlled by two ground operators and carry an explosive charge with which they accurately hit targets, tanks, artillery pieces, radio stations (Boussios, 2015, p. 44).

Potential benefits and risks. Like any military technology, drones have their own *advantages and disadvantages* regarding their use in combat.

Advantages. The latest research has shown that the weapon systems on board these drones are becoming even *smaller in size* and *more precise*. *Accuracy on target*, relative ease of use, *reduced* (human) *risk* and considerably *reduced costs* compared to other means with similar effect on target, as well as *the high cost* of protection against them make them *very effective capabilities*. Thus, a global proliferation of drones has been triggered very quickly (Boussios, 2015, p. 45). Detecting drones and protecting sensitive capabilities within military installations and base locations is a threat posed by the way drones operate. Automating some or all of the flight requirements of remotely controlled drones allows for significant cost savings and multiplies the effects on the target. In addition, autonomous systems are generally able to react substantially faster than operators (Lucas, 2016, p. 10). Drones make manoeuvring difficult and force troops and vehicles to remain

in shelter and fortifications, and FPV drones, guided by fibre optic cables, cannot be jammed.

The use of drones creates a situation in which the place of decisive human decision-making physically moves *outside the area of combat actions* and, at the same time, it is becoming increasingly characteristic that the decision, chronologically, is located quite *far from the moment of kinetic action* (Boussios, 2015, p. 44).

Among the relevant advantages can be mentioned: unmanned (low risk); capable of extended surveillance with autonomy; full-motion video (day or night); increases effectiveness and combat power; protection through real-time situational monitoring; both tactical and strategic platforms; capable of autonomous flight; capable of air-to-ground weapons launch; CAS – close air support; detection and neutralization – convoy security; signals intelligence collection (SIGINT); imagery intelligence collection (IMINT)/Ground Moving Target Indicator (GMTI); communications intelligence support (COMINT); electronic intelligence collection (ELINT); rapid response and target determination for indirect fire (IDF), ambush/troops in contact (TIC); high-value person targeting (HVI), and named/targeted area of interest (NAI/TAI) recognition (Wallestad, 2011, pp. 1-3).

Potential risks. The UN Charter, Art. 2, 44 and numerous international treaties prohibit the killing of persons on foreign territory, outside of an armed conflict, except in extraordinary circumstances. Drone attacks have a powerful effect on the adversary and create enormous short-term benefits, but the damage they cause to political alliances in the long term is worrying. The legal, authorized use of drones is conditioned by location and purpose. In the area of “*declared*” combat actions, the use of drones has clear rules of engagement. According to the UN Charter, Art. 51, countries can use force in self-defence. Article 2, paragraph (4) of the UN Charter prohibits the use of force (Boussios, 2015, p. 45).

The precision and accuracy of drone attacks are conditioned by *information from the ground* and its *timely transmission*. There have been situations when close-up video recordings of the effects of drone action have been made live. However, there are some doubts about whether: the targets were selected correctly, collateral damage was avoided and whether the on-board equipment provides images that correspond to the real description of the target. Even if the final result seems to be a success, it leaves a trace of doubt about how precise the confirmation of the target was: equipment or personnel, hostile (ib., p. 44).

Among the essential disadvantages can be mentioned: reinforcing the feeling of “*distant enemy*” or something else, creating a false image in public opinion

about the consequences of the war; questionable legality that further distances policy from practice; drone use reflects torture – a “*torturer*” harming a helpless victim, without any risk to himself –, created by the image of a drone operator in Langley firing on a target in Afghanistan, which differs from conventional armed conflict in which two adversaries pose a *similar level of threat* to the other; may be subject to cyberattacks or enemy interception; potential to foster domestic terrorism; data overload; lasting psychological effects on pilots due to lethal use on a video monitor (as if playing a video game) (Wallestad, 2011, pp. 1-3).

There are already drone interceptors, technology developed by Ukraine, the UK and other states – a technology that has proven “*extremely effective*” against the Shahed unidirectional attack drones and costs less than 10% of the cost of the Russian systems they destroy (Ruitenbergh, 2025, pp. 1-5).

Countering drones. Mobile counter-drone systems are being experimented with, which can be deployed, including by commercial aircraft, to respond to drone incursions, thus supplementing the sometimes difficult-to-implement multi-layered defences of military installations, including jamming, microwave and laser weapons, and kinetic weapons such as machine guns (Peck, 2025, pp. 1-6). Directed energy weapons (DEWs) (lasers and microwave weapons) complement kinetic weapons and will combat various emerging threats, such as *swarming drones*. While DEWs are best suited to combat drones for now, the use of laser weapons could represent a less expensive alternative to missile-based defences, which can be overwhelmed by multiple targets, against scenarios with swarms of small, inexpensive drones flying at low altitudes. Electronic warfare methods have also been used to block drone signals by jamming radio frequencies (Demarest, 2023, p. 4).

One of the main concerns with today’s non-autonomous remote-controlled weapons systems is represented by the issue of both insecure connections to the remote operator and the possibility of enemy interference. There is the possibility that the enemy could “*hack*” the computerized control systems frequently used for network communication (Lucas, 2016, p. 10). Many analysts believe that electronic warfare is the most effective defence against small drone variants. Defending military bases against drones is both a matter of law and a matter of technology. Responding to drone attack requires specific and explicit rules of engagement. There is an informal political agreement concluded in 1987, the Missile Technology Control Regime – to limit the proliferation of missiles and missile technologies – which also applies to certain unmanned aerial vehicles (drones) and obstructs the trade in drones with other states (Dent, 2025, p. 1).

CONCLUSIONS

Evaluating the use of drones in combat actions in recent conflicts, it results that they are very effective and efficient; drones that cost a few hundred dollars can neutralize expensive combat equipment – tanks, artillery pieces, radio-electronic stations or warehouses with stocks of vital materials to support the war – worth millions of dollars, which demonstrates their transformative role in modern warfare. To deal with a large number of drone incursions, especially small ones and in groups/swarms, simultaneously on multiple critical military installations and locations, militaries need more anti-drone technology and expanded authority to act against them, as well as accelerating the production of technologies to detect and destroy enemy drones. At the strategic level, drones provide the ability to substantially reduce personnel losses, financial costs, and public disapproval of the conflict, while at the operational level, they disrupt combat assurance measures, force manoeuvre, and logistic support.

The effects of using drones in combat determine the re-examination of the following aspects: the defence of forces, bases and strategic positions, providing rapid solutions with an emphasis on the detection, tracking and identification of threats, as well as active and passive defence. The following elements: keeping pace with advances in unmanned systems; clarifying, streamlining and delegating authority as necessary; adapting force doctrines; organizing, equipping, leading and training personnel; strategies for using and countering drones and deploying sufficient means of defence against attacks in swarms and simultaneously at multiple locations will contribute to achieving a competitive advantage.

The widespread use of drones in the war in Ukraine has led to an equally high demand for anti-drone equipment. *Directed energy weapons* represent an alternative option to expensive means of countering drones, an effective tool for defending against attacks by armed drones, which have been widely used in the Russo-Ukrainian war and other regional conflicts. Interceptor drones, state-of-the-art equipment, inexpensive compared to conventional drones and air defence missiles, are an effective option in countering waves of unidirectional attack drones.

BIBLIOGRAPHY:

1. Abdullah, Q.A. (2023). *Classification of the Unmanned Aerial Systems*, The College of Earth and Mineral Sciences, pp. 1-12, <https://www.e-education.psu.edu/geog892/node/5>, retrieved on 15 September 2025.
2. Becker, J. (30 June 2020). *When It Comes to Missiles, Don't Copy Russia and China – Leap-frog Them*, War On The Rocks, pp. 3-5, <https://warontherocks.com/2020/06/>

- when-it-comes-to-missiles-dont-copy-russia-and-china-leapfrog-them, retrieved on 15 September 2025.
3. Boussios, E. (January 2015). *Changing The Rules of War: The Controversies Surrounding the United States' Expanded Use of Drones* by Emanuel Boussios, in *Journal of Terrorism Research*, vol. 6, no. 1, pp. 1, 43, 44, https://www.researchgate.net/publication/282841299_Changing_The_Rules_of_War_The_Controversies_Surrounding_the_United_States'_Expanded_Use_of_Drones, retrieved on 15 September 2025.
 4. Brock, J. (21 September 2023). *U.S. revives Cold War submarine spy program to counter China*, Reuters, pp. 1-10, <https://www.reuters.com/investigates/special-report/usa-china-tech-surveillance/>, retrieved on 15 September 2025.
 5. Cagaptay, S. (27 April 2022). *Turkey's Lethal Weapon from Ukraine to Syria, Drones are Reshaping Erdogan's Foreign Policy*, Foreign Affairs, p. 1, <https://www.foreignaffairs.com/articles/turkey/2022-04-27/turkeys-lethal-weapon>, retrieved on 15 September 2025.
 6. Chiu, L. (11 September 2025). *UK to Produce Interceptor Drones for Ukraine – Shmyhal*, Kyiv Post Ukraine's Global Voice, pp. 1-9, <https://www.kyivpost.com/post/59925> retrieved on 15 September 2025.
 7. Demarest, C. (18 September 2023). *Directed energy weapons making jump from sci-fi to real world*, C4ISRNET, p. 4 (c4isrnet.com), retrieved on 15 September 2025.
 8. Dent, E. (17 September 2025). *How Washington's drone policy is catching up to reality*, in *Defense News*, https://www.defensenews.com/opinion/2025/09/16/how-washingtons-drone-policy-is-catching-up-to-reality/?utm_source=sailthru&utm_medium=email&utm_campaign=dfn-opinion, retrieved on 18 September 2025.
 9. DoD (December 2024). *Fact Sheet, Department of Defense Strategy for Countering Unmanned Systems*, pp.1-2, <https://media.defense.gov/2024/Dec/05/2003599149/-1/-1/0/fact-sheet-strategy-for-countering-unmanned-systems.pdf?sv=2019-07-07&ss=b&srt=o&spr=https&se=2024-12-07T16%3A01%3A14Z&sp=r&sig=mRFnyOqgDwaJkTXAbKPABnBYEsiOkk1zALn11v3ljYQ%3D>, retrieved on 15 September 2025.
 10. Drone wars (3 November 2022). *Twenty years of drone targeted killings*, p. 1, <https://dronewars.net/twenty-years-of-drone-targeted-killings/>, retrieved on 15 September 2025.
 11. Embry-Riddle (2022). *Aircraft Classifications & Regulations*, Embry Riddle Aeronautical University, pp. 1-26, <https://eaglepubs.erau.edu/introductiontoaerospaceflightvehicles/chapter/aircraft-classifications-aviation-regulations/>, retrieved on 15 September 2025.
 12. Franke, U.E. (23 August 2017). *Drone Warfare*, Oxford Bibliographies, pp. 1, 3-12, https://www.academia.edu/38170568/Drone_Warfare_Oxford_Bibliographies, retrieved on 15 September 2025.
 13. Gillis, A.S. (26 July 2024). *What is a drone (UAV)?* Tech Target Network, pp. 1-10, 16-20, <https://www.techtarget.com/iotagenda/definition/drone>, retrieved on 1 September 2025.
 14. Gosselin-Malo, E. (14 May 2024). *Ukraine, Russia race to shield battle tanks from exploding drones*, in *Defense News*, pp. 1-6, <https://www.defensenews.com/global/europe/2024/05/14/ukraine-russia-race-to-shield-battle-tanks-from-exploding-drones/>, retrieved on 15 September 2025.

15. Gosselin-Malo, E. (13 May 2025). *AI company Helsing unveils swarming underwater surveillance drones*, in *Defense News*, pp. 1-3, <https://www.defensenews.com/global/europe/2025/05/13/ai-company-helsing-unveils-swarming-underwater-surveillance-drones/>, retrieved on 15 September 2025.
16. Haqpan, S. (2013). *Does the advent of drones mark a fundamental change in the conduct of war?*, Academia.edu, pp. 1-5, https://www.academia.edu/45105943/Does_the_advent_of_drones_mark_a_fundamental_change_in_the_conduct_of_war, retrieved on 15 September 2025.
17. Höller, L. (31 July 2025). *Behind attacks on Ukrainian cities, Russia is building a drone empire*, Military Times, p. 1-3, 15-20, <https://www.militarytimes.com/global/europe/2025/07/31/behind-attacks-on-ukrainian-cities-russia-is-building-a-drone-empire/>, retrieved on 15 September 2025.
18. Horowitz, M.C. (20 November 2020). *China has Made Drone Warfare Global. The United States Must Join the Market or be Left Behind*, in *Foreign Affairs*, pp. 1-2, 14, <https://www.foreignaffairs.com/articles/china/2020-11-20/china-has-made-drone-warfare-global>, retrieved on 15 September 2025.
19. IWM, *A Brief History of Drones*, Imperial war museum (2025), pp. 1-12, <https://www.iwm.org.uk/history/a-brief-history-of-drones>, retrieved on 15 September 2025.
20. Karako, T. (23 December 2022). *Deterrence, Air Defense, and Munitions Production in A New Missile Age*, Strategika, Hoover Institution, pp. 1-7, 15-34, 36-43, 62, <https://www.hoover.org/research/deterrence-air-defense-and-munitions-production-new-missile-age>, retrieved on 15 September 2025.
21. Kunertova, D. (2021). *New Missiles, Eroding Norms, European Options after the Demise of the INF Treaty*, The Centre for Military Studies, pp. 55, 69, https://cms.polsci.ku.dk/publikationer/nye-missiler-udhulede-normer-europaeisk-sikkerhed-efter-inf-traktatens-ophoer/download-cms-rapport/CMS_Report_2021__4_-_New_missiles__eroding_norms.pdf, retrieved on 15 September 2025.
22. Lin-Greenberg, E. (20 December 2022). *The Dawn of Drone Diplomacy Unmanned Vehicles are up ending the Arms Trade – and the Balance of Power*, in *Foreign Affairs*, pp. 1-5, <https://www.foreignaffairs.com/ukraine/dawn-drone-diplomacy>, retrieved on 15 September 2025.
23. Losey, S. (2 September 2025). *Drones, AI and robotics challenge order of Top 100 defense firms*, Defense News, pp. 1-15, https://www.defensenews.com/industry/2025/09/02/drones-ai-and-robotics-challenge-order-of-top-100-defense-firms/?utm_source=sailthru&utm_medium=email&utm_campaign=dfn-special-report, retrieved on 15 September 2025.
24. Lucas, N.J. (14 April 2016). *Lethal Autonomous Weapon Systems: Issues for Congress*, Congressional Research Service, p. 10, <https://apps.dtic.mil/sti/trecms/pdf/AD1170011.pdf>, retrieved on 15 September 2025.
25. Lyall, J. (16 December 2020). *Global Politics, Simple Vehicles Make Conflict Tempting and Cheap*, in *Foreign Affairs*, p. 1, <https://www.foreignaffairs.com/articles/middle-east/2020-12-16/drones-are-destabilizing-global-politics>, retrieved on 15 September 2025.

26. Malkasian, C. (17 July 2025). *Nuclear Powers, Conventional Wars The Dangerous Erosion of Deterrence*, in *Foreign Affairs*, p. 1, <https://www.foreignaffairs.com/united-states/nuclear-powers-conventional-wars>, retrieved on 15 September 2025.
27. Miller, A.D. (9 September 2025). *U.S. Leadership in a Challenging World: A Conversation with Former CIA Director William J. Burns*, pp. 1-2, <https://carnegieendowment.org/events/2025/08/us-leadership-in-a-challenging-world-a-conversation-with-former-cia-director-william-j-burns?lang=en>, retrieved on 15 September 2025.
28. Peck, M. (14 August 2025). *China's military wants to target US under sea sensor network: Analysis*, *Defense News*, pp. 1-6, <https://www.defensenews.com/global/asia-pacific/2025/08/13/chinas-military-wants-to-target-us-undersea-sensor-network-analysis/>, retrieved on 15 September 2025.
29. Ruitenberg, R. (5 September 2025). *DSEI UK to show war's tech revolution, military adviser Waterfall says*, *Defense News*, pp. 1-6, https://www.defensenews.com/global/europe/2025/09/05/dsei-uk-to-show-wars-tech-revolution-military-adviser-waterfall-says/?utm_source=sailthru&utm_medium=email&utm_campaign=dfn-dnr, retrieved on 15 September 2025.
30. Sayler, K.M. (10 November 2020). *Artificial Intelligence and National Security*, Congressional Research Service, pp. 1, 13-16, 29, <https://sgp.fas.org/crs/natsec/R45178.pdf>, retrieved on 15 September 2025.
31. Secretary of Defense (10 July 2025). *Memorandum for Senior Pentagon Leadership Commanders of the combatant commands Directors of Defense Agencies*, pp. 1-5, <https://static.foxnews.com/foxnews.com/content/uploads/2025/07/unleashing-u.s.-military-drone-dominance-osd006689-25-res-final.pdf>, retrieved on 15 September 2025.
32. Shaw, I. (2014). *The Rise of the Predator Empire: Tracing the History of U.S. Drones*, *Understanding Empire: Technology, Power, Politics*, pp. 1, 6-8, 24, <https://understandingempire.wordpress.com/2-0-a-brief-history-of-u-s-drones/>, retrieved on 15 September 2025.
33. Shaw, I. (10 August 2028). *The Final Frontier: Enclosing Outer Space*, *Understanding Empire: Technology, Power, Politics*, pp. 1-5, <https://understandingempire.wordpress.com>, retrieved on 15 September 2025.
34. STANAG 4586 – *Standard Interfaces of UAV Control System (UCS) for NATO UAV Interoperability*, NATO S&T Organisation, 2014, p. 3-1, <https://publications.sto.nato.int/publications/STO%20Educational%20Notes/STO-EN-SCI-271/EN-SCI-271-03.pdf>, retrieved on 15 September 2025.
35. Tucker, P. (11 July 2025). *Drones are now bullets: How a new Pentagon policy may accelerate robot warfare*, *Defense One*, pp. 1-10, <https://www.defenseone.com/policy/2025/07/drones-are-now-bullets-how-new-pentagon-policy-may-accelerate-robot-warfare/406686/>, retrieved on 15 September 2025.
36. Tucker, P. (22 August 2025). *The Pentagon plan to Americanize drone warfare*, *Defense One*, pp. 1, 3-5, https://www.defenseone.com/technology/2025/08/pentagon-plan-americanize-drone-warfare/407625/?oref=d1-featured-river-secondary&utm_source=Sailthru&utm_medium=email&utm_campaign=The%20D%20Brief:%20August%2022%2C%202025&utm_term=newsletter_d1_dbrief, retrieved on 15 September 2025.

37. Vyas, K. (12 March 2025). *A brief history of drones: from pilot less balloons to roaming killers*, Interesting Engineering, pp. 1-25, <https://interestingengineering.com/innovation/a-brief-history-of-drones-the-remote-controlled-unmanned-aerial-vehicles-uavs>, retrieved on 15 September 2025.
38. Wallestad, J.D. (17 October 2011). *Drones: A New Chapter in Modern Warfare*, INEGMA, pp. 1-3, https://www.academia.edu/1019471/Drones_A_New_Chapter_in_Modern_Warfare, retrieved on 15 March 2025.
39. Zafra, M. (26 March 2024). *How drone combat in Ukraine is changing warfare*, Reuters, pp. 1, 3-15, <https://www.reuters.com/graphics/UKRAINE-CRISIS/DRONES/dwpkeyjwkpm/>, retrieved on 15 September 2025.

RECONFIGURING MARITIME AND RIVER OPERATIONS BY USING NAVAL DRONES

Commander Ioan MOLDOVAN

Romanian Naval Forces

DOI: 10.55535/RMT.2025.3.04

The use of naval drones in maritime and river operations requires an analysis of the combat space and innovative perspectives on future maritime security. This article aims to address a less explored issue, namely the effects of the use of naval drones on naval tactics. This scientific article uses online content analysis to identify the use of naval drones in maritime and river military actions, as well as the frequency of occurrence of the term naval drones or derivatives in the online environment. For this purpose, we have proposed the analysis of three situations, related to the use of drones in military and non-military actions, with the help of a tool to centralize Internet searches and observe trends in the field. The novelty of this article for the prospect of reshaping maritime and river operations using naval drones, and the potential repercussions lies in future maritime security. This approach addresses all maritime researchers and naval practitioners concerned with adapting naval tactics to the dynamics of capability development.

Keywords: reconfiguration of maritime operations; naval drones; USV; naval tactics; FPV;

INTRODUCTION

Reconfiguring maritime and river operations by using naval drones brings into question a different approach to naval tactics used for military actions in the maritime and driver areas, as well as for the protection of critical maritime infrastructure.

The scientific article addressed a problem less studied so far in national and international scientific papers, the effects of using naval drones on naval tactics, in the online environment, in the period 2022-2025.

During the online content analysis applied to the use of naval drones in conflicts, we felt the need to synthesize the information encountered on the 3 major regions, the Red Sea region, the South China Sea region and the Black Sea region, in order to exemplify and identify the specific maritime security features, as well as to conclude possible effects of the use of naval drones on tactics.

Regarding literature review, the authors S. Dumitrescu (2025) and P.C. Katoch (2021) present insights into the use of naval drones to protect critical maritime infrastructure, but do not address the possible effects of the use of naval drones on tactics.

Author Horton (2024), analyzes the prospect of developing Houthis rebel bases, but does not sufficiently address the use of naval drones and the effects on naval tactics of the fleets of the countries of the Red Sea region. The author Trevithick (2025) deals with the use of naval drones in the South China Sea region, but does not present possible effects on the naval tactics of the countries in the region.

Next I will present the research methodology and the structure of the article.

The main research objective of this article is the impact of the use of naval drones on tactics, as it appears online, in the period 2022-2025. The main research question that this article is trying to answer is: *What are the effects of using naval drones on tactics?*

In this context, the article was divided into two parts following a logical progression. Thus, initially, we exemplified three analysis situations from different regions and presented the impact of search interest in the online environment. Later, we compared the three situations and highlighted implications related to the research question.

Our scientific approach was empirical, using qualitative research. For the collection of data we used the online content analysis method, systematically analyzing online content to identify the frequency of occurrence of certain online words related to the use of naval drones. The results were mainly based on secondary data, the researcher having an important role in content analysis and interpretation of data of authors from the online environment. The research also used more than 70 websites that looked at the use of naval drones in military actions or against critical maritime infrastructure in the analyzed regions.

In the first part of the article, we used a tool to centralize Internet searches and trend observation, Google Trends, for searched topics specific to the use of naval drones in conflicts. As for Google Trends, we only used two tools to chart the level of search interest over a period and highlight the search interest by region. The chart includes values from 0 to 100, and the numbers represent the search interest associated with the highest point in the chart, for the specified region and time. The value of 100 represents the maximum popularity of the term in the period under investigation, and the score of 0 shows that not enough data are available for this term. Highlighting the search interest in the form of a world map has the following characteristics reported to the term of drone ships, thus: keeps the same scale of score from 0% to 100% and highlights with blue color and according to popularity, higher probability of the term sought. Obtained charts and highlighted maps are screenshots of the Google Trends app for the subject being searched in the desired period.

In the second part of the article we used searches of nominal phrases, nominal expressions and nominal groups in indexed databases and Google search engine for the investigated subject, as follows: houthis pirates, houthis, underwater drones China, Crimean bridge, Ukrainian naval drones and other derivatives of naval drones, USV, UUV, FPV.

We will continue to highlight the limits of research. In the first part, charts that highlight the search interest can be influenced by the Google Trends tool, which highlights the search interest according to the number of inhabitants of a country. Consequently, small countries are most often highlighted more strongly on the world map influencing the icons obtained. In the second part, not having enough data available from scientific articles, we turned to online sites to identify the possible effects of the use of naval drones on tactics and, implicitly, on the critical maritime infrastructure of the states in the analyzed regions.

USE OF NAVAL DRONES ON CRITICAL MARITIME INFRASTRUCTURE

In this first part, we will present the impact of the use of naval drones on tactics and critical maritime infrastructure, as it appears online, after 2022 so far, from the regions of the Red Sea, South China Sea and Black Sea.

The scientific approach analysed several bibliographic sources on the Internet in order to identify the impact of the use of naval drones on naval tactics and, implicitly, on critical maritime infrastructure at global level, in order to identify the countries interested in the subject and the search interest from 2022 to the present.

Red Sea Region

In the Red Sea Region, our research has identified kamikaze surface naval drones owned by non-state actors, the Houthis rebels. Naval drones have been used in maritime terrorism actions on merchantships and military vessels since 2017. The most plausible example in this region is the hit of a Saudi frigate by a kamikaze naval drone by the Houthis rebels in 2017. The naval drones struck the frigate behind the superstructure with the aim of damaging propulsion and governance (Arabia, 2017). Following this attack on the frigate, the ship and helicopter located on the deck were taken out of operation. In this region, the Houthis rebels affected the security of maritime communication lines at regional and international level by executing numerous attacks on merchant ships (Aljazeera, 2019). Moreover, the Houthis rebels, from the time of the declaration of support for the Hamas group involved in the Gaza War on 7 October 2023 to the end of 2024, engaged a substantial number of merchant ships of about 134, with missiles, air drones and naval drones executing direct strike missions, for the incapacity crossing of ships transiting the Red Sea (Horton 2024, pp. 15-22).

On 12 June 2024, about 66 Mm southwest of Yemen's Al Hudaydah port, the Houthis rebels engaged a merchant ship by using a combined kamikaze surface naval drone from the stern of the ship in order to reduce the ship's manoeuvring capacity, and then by launching a missile towards the target (UKMTO, 2024). Following the attack, the ship was captured by the Houthis group and transported to the nearest port.

Another notable attack, on 6 July 2025, about 51 Mm southwest of Yemen's Al Hudaydah port, occurred on a swarm of surface kamikaze naval drones, grenade launchers on board fast and military assault weapons boats attacked a merchantship

(UKMTO, 2025). Following the attack, the ship was hit by two naval drones on board the port and was sunk.

The last report on the Internet from 2022-2025 on the level of interest of the topic houthis pirates according to Google Trends is as follows:



Numbers are the search interest associated with the highest point in the chart, for the region and the specified time. The value of 100 represents the maximum popularity of the term. The value of 50 shows that popularity is half of the maximum recorded. Score 0 shows that not enough data is available for this term (Google Trends, 2022-2025).

The diagram above shows a massive increase in search interest related to the subject under investigation during October 2023 – January 2024, following repeated attacks by houthis rebels on merchant ships transporting goods to Israel as a protest against the Gaza War (Duggal, Haddad, 2024). In the aforementioned period of maximum interest, about 6 months, 40 merchant ships were attacked by the houthis rebels in the waters of the Red Sea. The other periods coincide with attacks on commercial ships using kamikaze drones, helicopters, missiles and aerial drones.

The internet search interest related to houthis pirates, Belgium holds the first position followed by the US countries, Australia, the United Kingdom, the Netherlands, Canada and India, probably the countries interested in international transport and trade.



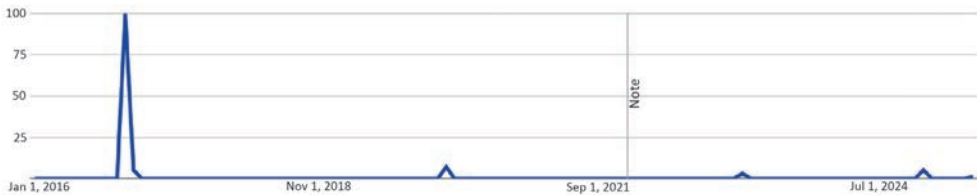
The conclusion of this research is related to a spectacular media impact, the intervention of non-state actors in the control of the Red Sea, the direct hit of a military ship with naval drones, direct engage of merchant ships with naval drones, missiles and aerial drones, a concern of NATO countries and countries in the region to restore maritime security, suspicious activities regarding the identification of the rhythm of activities, and possible implications of some state actors in support of the Houthis rebels, piracy activities and maritime terrorism activities (SANA'A Center for Strategic Studies, 2022).

South China Sea Region

Underwater naval drones in the South China Sea region have been used under military tensions related to territorial disputes since 2016 (Berglund, 2017).

In the South China Sea region, as early as 2016, there were some underwater drones of Chinese origin that were used in experimental research (Katoch, 2021).

Following the research of several sites from 2016 to date on the level of interest of the subject underwater drone China according to Google Trends, the report is as follows:



Search interest in December 2016 is marked by a global increase in internet searches at a rapid rate of breaking news, and in the other periods only small increases related to finding other Chinese underwater drones (Ib.). The diagram above highlights a massive increase in search interest related to the subject under investigation in December 2016, as an underwater drone was found near Quang Ngai in Vietnam in November 2016 (Swarajya, 2021). Therefore, on 20 December 2020, near the islands of Selayar, Indonesia, a drone was found (Trevithick, 2025), several Chinese underwater research drones were launched in mid-2023 (IntelligenceOnline, 2023), as well as finding a Chinese drone on 30 December 2024 near the coast of Philippines (Trevithick, ib.).

The timing of finding Chinese underwater drones has been marked by remarkable search interest in Singapore, the Philippines, the USA, Australia, India, Canada and the UK, according to Google Trends (Google Trends, 2022-2025).



Therefore, research in the South China region highlights a media impact such as breaking news for finding Chinese drones (Tsering 2016, p. 1). Also, there is a high search interest of the countries in the competition for the hegemony of the world by USA, Canada and India, but also of the countries bordering the South China Sea that are in permanent uncertainty – Singapore, the Philippines and Vietnam (VnExpress, 2023). Moreover, the use of underwater drones in passive mode could pose a threat to transport capabilities and routes in the region (Trevithick, ib.).

Black Sea Region

In the Black Sea region, surface, underwater and aerial naval drones are used in the war in Ukraine on both the Ukrainian side and the Russian side to attack critical maritime infrastructure.

Following the research of several sites from 2022 to date on the level of interest of the topic *Crimean bridge* according to Google Trends (Trends, 2022-2025), the report is as follows:



Analyzing the diagram above and taking into account the military events of the analyzed period, we note that the periods of maximum interest of the subject coincide with the attacks of Ukrainian drones on the bridge in Crimea (Goldsmith, 2025). Accordingly, on October 8, 2022, at the top of the diagram's audience, the bridge was the target of a Ukrainian truck loaded with explosives, which led to the burning of a train with fuel tanks on the bridge at the time of the explosion (Kropman, 2022). Moreover, some observers identified surface naval drones on video footage

seconds before the explosion and considered the bridge to be the target of an explosion below the bridge, most likely caused by kamikaze surface drones (Adams, 2022). Another event recorded on the diagram on July 17, 2023, was damage to the bridge in the Kerch Strait with Ukrainian naval drones (Pennington et al. 2023). In 2025, the Crimean bridge was once again the target of naval drones, this time even if surface naval drones were neutralized, most likely the explosion was produced by underwater naval drones (Yan, 2025). The diagram also highlights other increased levels of interest that coincide with media promotion campaigns and the spread of other attacks carried out with Ukrainian naval drones or Russian naval drones.

In February 2023, there is a new increase on the diagram, this time Russia responded in a similar way, attacking a bridge near Odessa with a naval drone (James, 2023). According to Ukrainian publications, Russian naval drones have been the result of cooperation between the French company ECA Group and the Russians since 2017 in order to equip the mine sweepers (Sinitsyn, 2023).

Moreover, on August 28, 2025, the Russian navy for the first time organized a kamikaze naval drone attack on the Danube river, on the Chilia branch, 3 kilometers from the Romanian town of Periprava, in order to hit the Ukrainian ship Simferopol (Defense Romania, 2025). Following the attack, the ship was sunk and the Russian took revenge on the Ukrainian with the same type of kamikaze drone that lost almost half of Russia's Black Sea Fleet.

In the representation below are highlighted over 70 countries around the world marked by an interest in the remarkable search for the subject under investigation, and in particular, this is due to the fact that the bridge in Crimea is the symbol of Russian power at the Black Sea and of Ukrainian attempts to destroy this critical maritime infrastructure for the inhabitants of the Crimean peninsula.



Regarding the search trends of the subject, most likely it represents the interest of researchers in the field of naval drones, naval forces military personnel, all those interested in the use of naval drones in military conflicts, interest in the evolution of war, concerns about the evolution of war and concerns about the prolongation of war with global effects.

Moreover, in the Black Sea region, following the research of the nominal phrase Ukrainian naval drones, several online sources have been discovered that present the use of naval drones together with other vectors or other types of drones. For example, on 10 November 2023, surface naval drones together with aerial drones and missiles carried out attacks on Feodosia, as well as on ships in the port of Chornomorske (Rybar, 2023). In this case, the role of aerial drones was to distract the opponent and execute the drone attack on the surface. Another example, on 07 August 2025, Ukrainian surface drones have transported and launched several First Person Viewed (FPV) drones hundreds of nautical miles away from Ukraine, near the shore, in order to act to neutralize a Russian air defense radar (Stewart, 2025).

In conclusion, there search in the Black Sea region on the use of naval drones on naval tactics and implicitly on critical maritime infrastructure highlights a great global search interest, increasing capabilities with the daily prolongation of the Russian-Ukrainian war, capabilities used more and more frequently in all operating environments to capture the enemy a concern for both camps to use multiple naval drones in war, the use of kamikaze naval drones in the maritime an driver areas, and last but not least the use of drones to destroy or damage critical maritime infrastructure.

DISCUSSIONS AND IMPLICATIONS

In this part, we will turn our attention to the comparative analysis of the situations studied in the first part, we will present the resulting implications to the research question and possible implications in the Black Sea region.

Comparative analysis of the situations studied

In this part, we will review the studied situations and compare situations with each other. Therefore, the analysis of situations is carried out by highlighting the important elements, capturing the use of drones on critical maritime infrastructure, as well as their interpretation.

In the table 1, we find a brief presentation of the important elements of each studied situation, as follows.

Table 1: Overview of the analyzed situations (author's conception)

	Situation no. 1 Red Sea Region	Situation no. 2 South China Sea Region	Situation no. 3 Black Sea Region
Period	2022-2025	2016-2025	2022-2025
Actors involved	The rebels houthis and Israel	China and riparian countries: Singapore, Philippines, Vietnam	Ukraine and Russia
Causes	The Gaza war Offensive activities to engage illegitimate targets/ Undeclared	Tatonism and territorial disputes	The war in Ukraine Offensive activities to engage legitimate/declared targets
Critical Maritime Infrastructure deteriorated	Sea lines of communication	Sea lines of communication (SLOC)	Natural gas extraction platforms Road and rail bridges
Types of drones utilised	Kamikaze surface naval drones	Underwater marine research drones	Unmanned surface vehicle (USV) Unmanned aerial vehicle (UAS), ISR Drones, Unmanned underwater vehicle (UUV)
Media Impact	Spectacular media impact (7 regions)	Breaking news impact (7 regions)	Global impact (74 regions)
Lessons identified	- Concerns of NATO countries and countries in the region - Aggressive activities of control of SLOC	- High interest countries USA, India, Canada - Territorial disputes - Uncertainty countries bordering Singapore,	- Use of naval drones for the transport of other FPV drones - Territorial claims -International implications

	Situation no. 1 Red Sea Region	Situation no. 2 South China Sea Region	Situation no. 3 Black Sea Region
Period	2022-2025	2016-2025	2022-2025
	- Possible implications of some state actors - Activities of piracy - Maritime terrorism activities	- Philippines, Vietnam - Possible threats capabilities in the region - Possible threats to transport routes in the region	- Distraction of the opponent's attention - Neutralization of radars and essential sensors - Destroying essential sensors
Effects of the use of naval drones	- Piracy actions - Actions of maritime terrorism - Direct actions of employment of ships - Vulnerability of SLOC - Economic losses at global level	- Manoeuvres for the inspection of underwater structures - Mapping the seabed around critical maritime infrastructure - Possible sabotage actions for intimidation and deterrence.	- Definition of operational environment - Description of the influence of the information environment - Assessment of the opponent - Distraction of the opponent's attention - Destroying essential sensors - Damaging CMI - Destroying targets - Neutralization of radars and sensors essential for air defense systems, ships or OFF-shore platforms - Espionage actions

Regarding the comparative analysis of the studied situations, we turn our attention to the first two situations. If in the first situation under consideration the actions of naval drones are direct actions of piracy and maritime terrorism, with no declared intention over a short period of time with direct effect on maritime communication lines, in these situation drones carry out maritime research actions over a long period of time, which could have implications on maritime communications capabilities or lines. If in the first situation the drones were used for piracy and affecting the propulsion of commercial vessels near the sea communication lines, in these situation, the drones failed on the coast of the riparian countries and then they aroused questions.

As regards the comparative analysis of the first situation with the third situation, we identify notable differences regarding the protest or support approach, for the Hamas group, of the use of drones in the first situation, in grey areas or in international waters of the states, instead in the third situation, during war time, naval drones are used in the territorial waters of the adverse country with declared intentions of hiring critical maritime infrastructure.

Regarding the comparative analysis of these situation with the third situation, we identify clear differentiation of the use of drones. If in these situation, the drones were used in passive mode, foul mode and sabotage mode, in the third situation the drones were actively used in combinations with other vectors to engage the declared targets.

Implications Related to the Research Question

In this part, we will present the implications of the use of drones related to the research question stated at the beginning of the article – *What are the effects of the use of naval drones on naval tactics?* For this, we will briefly outline the resulting implications and their interpretation.

The surface naval drones used in the Red Sea region could be the result of actions by some state actors in order to destabilize the regional situation by supporting and encouraging some rebels or paramilitary groups to carry out piracy actions and actions of maritime terrorism. Moreover, the naval drones were engaged in direct actions to hit the merchant vessels for the passage in a state of reduced maneuverability, inability to maneuver and until the sinking of the ships. Following the research, it emerged that naval drones could be used to destabilise international freight transport. Consequently, it could have a considerable impact on the vulnerability of communication lines by avoiding this region and choosing longer

shipping routes (Duggal, Haddad, 2024). Therefore, the actions of surface drones used in the Red Sea region could influence the missions of NATO, USCENTCOM, China and the countries of the region, from tactical to strategic level. On a tactical level, military fleets involved in the protection of merchant ships transiting the Red Sea should most likely reconsider capabilities capable of countering multiple threats from the Houthis rebels and only send ships capable of handling threats from surface kamikaze naval drones. On a strategic level, international authorities should probably set up operations to protect containers destined for Europe, provide military support to vessels transiting this region and support the establishment of regional coalitions for the protection of trade of partner states (Aljazeera, 2019). Moreover, the research highlighted the emergence of state actors such as China, which condemn actions against houthis rebels and be able to provide protection to merchant ships.

The naval drones used in the South China Sea could be the result of China's explorations and threats to riparian countries on territorial disputes and the substantial increase in manoeuvres for inspection of underwater structures, mapping the seabed around infrastructure, possibly sabotage with the aim of intimidation and deterrence. All of these possible effects could provide China with advantages in the event of a conflict to define the operational environment or to identify vulnerabilities of critical maritime infrastructure and underwater cable networks.

Naval drones used in the Black Sea region are diversified and adapted for all operating environments, from aerial naval drones, naval drones to surface and under water naval drones. The wide spread use of drones in the Russian-Ukrainian war could be the result of technological evolution, adaptation of the technique to meet the needs of war, as well as for damage to adverse critical maritime infrastructure. The naval drones carried out missions in support of the special research forces of the theater of operations with the purpose of defining the operational environment, describing the influence of the information environment, assessing the adversary and espionage ctions. The drones also carried out missions in support of other capabilities in order to distract attention from objectives of great importance or to deceive the opponent through direct attacks on the essential sensors deployed on critical maritime infrastructure. Moreover, the drones were operated in several environments executing direct attacks for damage to critical maritime infrastructure, target destruction and military neutralization on board OFFSHORE platforms.

Other possible effects of the use of naval drones on tactics could be the detection of adverse ships, patrols in certain districts, detection of submerged capabilities or transport of equipment.

Russia's naval tactics were heavily affected by the attack of Ukrainian naval drones on the Russian Navy at the Black Sea. At the beginning of the war in Ukraine, Russian forces acted to control the sea and even deny the use of the sea by Ukrainian forces. Due to the prolongation of the war in Ukraine, Russian naval forces began to erode, unable to sustain the war effort and even become targets. Following the assessment of the action of naval drones, Russian forces were most likely determined to place much greater emphasis on the near defense of ships, to act vigilantly for the employment of naval drones, to increase the safety area of combat ships against the shoreline, as well as to withdraw military vessels to the eastern Black Sea.

The naval tactics of the world's fleets in the maritime and river areas require urgent adaptation to this military phenomenon, naval drones, given the effects of the use of naval drones by non-state or state actors from the tactical level to the strategic level. The possibilities of using naval drones from simple platforms operating in a single operating environment to drones that can operate in multiple environments in support of means and combat forces or supported by other capabilities must also be explored.

Implications for Romania

In Romania, critical maritime infrastructure is an important component of energy production, resource exploitation, power projection at sea or the maintenance of free maritime communication lines connected to international trade. At the heart of the critical maritime infrastructure in Romania, the Neptun Deep project will most likely be. A project for the exploitation of natural gas resources in the exclusive economic area of Romania interconnected with the impressive under water infrastructure for the transport of resources through the network of under water cables and pipes that will be created for the transport of gas to shore (OMVPETROM, 2025). In the face of this ambitious project, there are already many challenges. For example, in the summer of 2022, Russian ships approached the natural gas extraction platform "Ana", in a suspicious way, raising many questions about the future of the security of Black Sea platforms (Profit.ro, 2023). There are also some authors who highlight the possibility of using future autonomous surface vehicles (MAVs) and aerial drones (UAVs) in research or sabotage of underwater

infrastructure (Dumitrescu, 2025, pp. 6-7). On the other hand, there are some authors who believe that surface naval drones could be used to protect critical maritime infrastructure (Manailă, Dogaru, 2024).

Following the research carried out, failed kamikaze naval drones were identified or whose command and control was lost during the mission on the maritime communication lines in the Black Sea. For example, in the contiguous area of Romania was found a first failed naval drone (Dumitrache, 2024), but whose origin was not disclosed. According H.I. Sutton, a defence analyst and open source investigative reporter (OSINT), the identified boat was of American origin with a cargo of about 500 kg of Soviet production (Sutton, 2024). The second explosive-loaded kamikaze naval drone was found drifting off the coast of the district of Catalca, near Istanbul (Newdick, 2024). Moreover, on 01 October 2025, a failed kamikaze surface naval drone was found in eastern Turkey, near the city of Karshibasi (Altman, 2025). In this case, the Ukrainian naval drone of Magura V type was end owed with explosive charge or other types of weapons and ammunition. Mostlikely, following the recovery of the drone carefully by some Turkish fishermen, the Turkish authorities will examine in detail the drone found (War_Noir, 2025). All these naval drones can have effects on the maritime communication lines in the Black Sea, implicitly on international trade, but also on the military fleets of the riparian countries that need to increase their vigilance, observation and close defense of the ships to counter the threat.

In the Black Sea, there are regional maritime patrol and surveillance initiatives to identify the threats of drifting mines on the critical maritime infrastructure of the countries Bulgaria, Turkey and Romania (Ministerul Apărării Naționale, 2024). Moreover, in the Black Sea, in terms of ensuring the protection of critical maritime infrastructure, there are several key elements that support each other from the presence of capabilities at sea, to information for defense and to the protection of cyberspace, with a role in avoiding communication paralysis and the deterioration of energy systems (Dumitrescu, pp. 20-22).

The naval tactics of the Romanian Naval Forces, most likely, should be adapted to new technologies, by equipping and integrating naval drones in the missions of the maritime and river component. Naval drones could be used in combat, from stand still, in hidden positions in the river area or in proximity to critical maritime infrastructure, from where to be operated to order against the capabilities of a possible enemy. Naval drones could also be used in combat, from mobile positions,

in an offensive way, either from the coast or launched from port-drone platforms or used in an ingenious way, to put real problems to a state superior technological and numerical aggressor.

CONCLUSIONS

Our scientific approach, through online content analysis, applied to the phenomenon of naval drones in correlation with critical maritime infrastructure, answers the research question by identifying the possible effects of the use of naval drones on naval tactics.

The scientific paper has analyzed several bibliographic sources on the Internet in order to identify the impact of the use of naval drones on global tactics since 2022.

Following the study of the use of naval drones on tactics and implicitly on critical maritime infrastructure, in the three regions and in the more than 70 sites, a remarkable media impact coincided with the disclosure of the use of drones in support actions or in direct actions, a growing global search interest and an exponentially growing capability with the daily prolongation of the war in Ukraine.

The impact of the media is probably more spectacular, in the Black Sea region, because a war between two states that claim territories is ongoing, there are international implications and last but not least, the intervention of the Western states in the war in Ukraine amplifying the interest of searching for the topic researched in the online environment.

The wide spread use of drones in the Russian-Ukrainian war could be the result of technological evolution, the adaptation of the technique to meet the needs of war, as well as for the mutual damage of opponents, in particular the damage to critical maritime infrastructure.

The effects of the use of naval drones on tactics are diversified and highlighted in all operating environments, from suspicious actions without declared intention over a short period of time to maritime research actions over a long period of time, from actions in grey areas or international waters to actions in territorial waters, from passive actions to direct employment actions.

The naval tactics of the Romanian Naval Forces most likely require an improvement and adaptation of the mission execution, by using naval drones both in support of the Maritime Fleet and in support of the River Flotilla.

The Black Sea remains a hot space of military confrontations with countless challenges and threats for the critical maritime infrastructure in Romania

and implicitly for the Romanian Naval Forces, the Coast Guard or the Maritime Authorities.

In conclusion, naval drones through the possibilities of action and autonomy implemented by state or non-state actors in international waters or territorial waters can have considerable impact on naval tactics either in offensive actions or defensive actions.

BIBLIOGRAPHY:

1. Adams, P. (2022). *Crimean bridge: Who - or what - caused the explosion?*, <https://www.bbc.com/news/world-europe-63192757>, retrieved on 2 August 2025.
2. Aljazeera (19 September 2019). *Saudi-led coalition intercepts explosive-filled boat 'by Houthis'*, <https://www.aljazeera.com/news/2019/9/19/saudi-led-coalition-intercepts-explosive-filled-boat-by-houthis>, retrieved on 11 September.
3. Altman, H. (30 September 2025). *Explosive-Packed Ukrainian Drone Boat Found 900 Miles Away In Turkey*, <https://www.twz.com/news-features/explosive-packed-ukrainian-drone-boat-found-900-miles-away-in-turkey>, retrieved on 2 October 2025.
4. Arabia, Government of Saudi (2017). *Houthi USV strike on a Saudi frigate operating in the Red Sea*. Editor Al Arabiya, https://www.youtube.com/watch?v=1kGJ_4aJTbE&t=41s, retrieved on 1 October 2025.
5. Berglund, P. (1 June 2017). *Territorial Disputes In The South China Sea: What You Need To Know*, <https://www.xeneta.com/blog/south-china-sea-dispute>, retrieved on 24 September 2025.
6. DefenseRomania (29 August 2025). *S-au „ascuns” dronele ruse în apele României înainte de a scufunda nava ucraineană Simferopol?*, https://www.defenseromania.ro/s-au-ascuns-dronele-ruse-in-apele-romaniei-inainte-de-a-scufunda-nava-ucraineana-simferopol-de-ce-e-imposibil-ca-rusii-sa-nu-fi-intrat-in-apel-e-teritoriale-romane_635547.html, retrieved on 1 October 2025.
7. Duggal, H., Haddad, M. (27 April 2024). *Mapping the Red Sea attacks*. ALJAZEERA, <https://interactive.aljazeera.com/aje/2024/mapping-red-sea-shipping-attacks/>, retrieved on 15 September 2025.
8. Dumitrache, C. (5 April 2024). *Drona navală eşuată în apele teritoriale româneşti a fost transferată în poligonul de la Capu Midia*, https://www.defenseromania.ro/drona-navala-esuata-in-apele-teritoriale-romanesti-a-fost-transferata-in-poligonul-de-la-capu-midia_627720.html, retrieved on 9 September 2025.
9. Dumitrescu, S. (2025). *Protecting Critical Maritime Infrastructure in the Black Sea*. Bucureşti: New Strategy Center.
10. Goldsmith, A. (3 June 2025). *Crimea bridge reopens after Ukraine says it carried out underwater explosion*, <https://www.bbc.com/news/live/cr58e9yr2ezt>, retrieved on 2 August 2025.
11. Google Trends 2022-2025, <https://trends.google.com/trends/explore?date=today%205-y&q=houthi%20pirates&hl=ro>, retrieved on 2 August and 21 September 2025.

12. Horton, M. (2024). *“Looking West: The Houthis’ Expanding Footprint in the Horn of Africa”*, CTC Sentinel, https://ctc.westpoint.edu/wp-content/uploads/2024/12/CTC-SENTINEL-112024_article-3.pdf, retrieved on 1 October 2025.
13. IntelligenceOnline (18 July 2023). *China deploys underwater reconnaissance drones in South China Sea*, <https://www.intelligenceonline.com/surveillance--interception/2023/07/18/china-deploys-underwater-reconnaissance-drones-in-south-china-sea,110004506-art>, retrieved on 31 August 2025.
14. Katoch, P.C. (19 July 2021). *China’s Underwater Drones*, <https://www.spsnavalforces.com/experts-speak/?id=456&h=Chinas-Underwater-Drones>, retrieved on 4 August 2025.
15. Kropman, V. (8 October 2022). *Взрыв на Крымском мосту мог стать результатом диверсии*, <https://www.dw.com/ru/vzryv-na-krymskom-mostu-mog-stat-rezultat-om-diversii/a-63376818>, retrieved on 2 August 2025.
16. Liam, J. (12 February 2023). *Russia strikes key Ukraine bridge with naval drone in attack feared to spell trouble for Kyiv’s navy*, <https://www.independent.co.uk/news/world/europe/russia-ukraine-drone-odesa-latest-b2280483.html>, retrieved on 7 September 2025.
17. Manailă, M., Dogaru, A. (2024). *Strategies XXI - Proceedings 2024. The 20th International Scientific Conference*. București: Editura U.N.Ap., <https://www.strategii21.ro/A/2024-04.%20TECHNOLOGIES%20-%20MILITARY%20APPLICATIONS%20SIMULATION%20AND%20RESOURCES/STRATEGIES%20XXI%20-%20TECHNOLOGIES%20%E2%80%93%20MILITARY%20APPLICATIONS,%20SIMULATION%20AND%20RESOURCES.pdf>, retrieved on 6 August 2025.
18. Ministerul Apărării Naționale (2024). *Comunicatul nr. 6*, https://www.mapn.ro/cpresa/18251_semnarea-memorandumului-de-intelegere-privind-constituirea-grupului-operativ-pentru-combaterea-minelor-marine-in-marea-neagra, retrieved on 28 August 2025.
19. Newdick, Th. (25 July 2024). *Explosives-Packed Jet Ski Drone Appears Off Turkish Coast*, <https://www.twz.com/sea/explosives-packed-jet-ski-drone-appears-off-turkish-coast>, retrieved on 9 February 2025.
20. NV, The new voice of Ukraine (29 July 2025). *Military Intelligence shows historic first-ever sea drone attack*, <https://english.nv.ua/nation/ukraine-s-first-use-of-fpv-drones-in-open-waters-revealed-50533193.html>, retrieved on 3 August 2025.
21. OMVPETROM (2025). *Neptun Deep: a stronger Romania*, <https://www.omvpetrom.com/en/our-business/exploration-and-production/neptun-deep>, retrieved on 6 August 2025.
22. Pennington, J., Stambaugh, A., Lendon, B., Edwards, C. (17 July 2023). *Ukraine claims responsibility for new attack on key Crimea bridge*, <https://edition.cnn.com/2023/07/16/europe/russia-crimea-bridge-intl-hnk>, retrieved on 2 August 2025.
23. Profit.ro. (8 March 2023). *Războiul Rusiei împotriva Ucrainei: Nave rusești, dar și o mină s-au apropiat periculos de cea mai nouă platformă petrolieră românească din Marea Neagră*, <https://www.profit.ro/povesti-cu-profit/energie/video-foto-razboiul-rusiei-impotriva-ucrainei-nave-rusesti-dar-si-o-mina-s-au-apropiat-periculos-de-cea-mai-noua-platforma-petroliera-romaneasca-din-marea-neagra-21047639>, retrieved on 6 August 2025.

24. Rybar (2023). *Атака ВСУ на Черноморское и Феодосию*, <https://t.me/rybar/54076>, retrieved on 19 September 2025.
25. SANA'A Center for Strategic Studies (October 2022). *Houthi Strikes Prompt Government Terrorism Designation*, <https://sanaacenter.org/the-yemen-review/october-2022/19003>, retrieved on 6 September 2025.
26. Sinitsyn, N. (13 February 2023). *Враг получил из Франции морские дроны-камикадзе? Чем оккупанты поразили мост под Одессой*, <https://telegraf.com.ua/tehnologii/2023-02-13/5779089-vrag-poluchil-iz-frantsii-morskie-drony-kamikadze-chem-okkupanty-porazili-most-pod-odessoy/amp>, retrieved on 7 September 2025.
27. Stetson P., Altman, H., Rogoway, T. (29 October 2022). *The War Zone*, <https://www.twz.com/ukraine-unleashes-mass-kamikaze-drone-boat-attack-on-russias-black-sea-fleet-headquarters>, retrieved on 10 September 2025.
28. Stewart, P. (7 August 2025). *Ukraine's GUR carried out a series of drone strikes on Russian air defense radars and other high value targets in Crimea*, https://x.com/prestonstew_/status/1953406791473086739?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1953406791473086739%7Ctwgr%5Edc2a842ba21b3d7f5494a4304d48e1812e26120d%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.twz.com%2Fnews-features%2Fcrewed-boa, retrieved on 1st October 2025.
29. Sutton, H.I. (8 April 2024). *Sea Drone Found in Black Sea is American Boat with Massive Soviet Warhead*, <https://www.navalnews.com/naval-news/2024/04/sea-drone-found-in-black-sea-is-american-boat-with-massive-soviet-warhead/>, retrieved on 9 September 2025.
30. Swarajya, S. (22 January 2021). *Explained: Why China Is Deploying Underwater Drones Near Indian Ocean Choke Points*, <https://swarajyamag.com/defence/explained-why-china-is-deploying-underwater-drones-near-indian-ocean-choke-points>, retrieved on 24 September 2025.
31. Trevithick, J. (2 January 2025). *Chinese Underwater Sea Glider Drone Caught By Fisherman In The Philippines*, <https://www.twz.com/sea/chinese-underwater-sea-glider-drone-caught-by-fisherman-in-the-philippines>, retrieved on 31 July 2025.
32. Tsering, D. (30 September 2016). *"China's Undersea Glider Haiyi - 7000: An Assessment"*. National Maritime Foundation, <https://maritimeindia.org/wp-content/uploads/2021/02/CHINAS-UNDERSEA-GLIBER-HAIYI-7000.pdf>, retrieved on 29 September 2025.
33. UKMTO (12 June 2024). *UKMTO WARNING INCIDENT 083 ATTACK UPDATE 003*, <http://ukmto.org/indian-ocean/ukmto-products/warnings/2024>, retrieved on 1st October 2025.
34. UKMTO (6 July 2025). *UKMTO_WARNING_INCIDENT_026-25 - ATTACK Update 001*, ukmto.org/-/media/ukmto/products/20250706-ukmto_warning_incident_026-25-update-01.pdf?rev=2d99509ab175442192367901ba27c132, retrieved on 1st October 2025.
35. VnExpress (16 December 2023). *A drone-like device drifted ashore in Quang Ngai*, <https://www.vietnam.vn/en/thiet-bi-giong-may-bay-khong-nguoi-lai-troi-vao-bo-bien-quang-ngai/>, retrieved on 29 September 2025.

36. War_Noir (30 September 2025). *Turkish Fishermen reportedly discovered an Explosive-Laden Uncrewed Surface Vehicle in #Trabzon, #BlackSea*, https://x.com/war_noir/status/1973047892400378281?ref_src=twsrc%5Etfw%7Ctwcamp%5Etwetembed%7Ctwterm%5E1973047892400378281%7Ctwgr%5E900e780c188f2b47c39bde691d7ac2b04448271d%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.twz.com%2Fnews-features%2Fexplosive-packed, retrieved on 2 October 2025.
37. Yan, O. (3 June 2025). *Magura naval drones were involved in the attack on the Crimean bridge*, <https://militaryni.com/en/news/magura-naval-drones-were-involved-in-the-attack-on-the-crimean-bridge/>, retrieved on 2 August 2025.

THE IMPACT OF ARTIFICIAL INTELLIGENCE ON CONTEMPORARY MILITARY ART – ADVANTAGE OR VULNERABILITY –

Colonel Florin ȘTEFĂNESCU

Colonel Dănuț-Gabriel DĂNILĂ

Lieutenant Colonel Nicolae-Cristian BRÂNZEIU

Major Nelu-Sorin DONEA

Captain Paul-Vasile HOSU

4th Infantry Division "Gemina", Cluj-Napoca

DOI: 10.55535/RMT.2025.3.05

This study aims to analyse the impact of emerging technologies, particularly artificial intelligence (AI), on the military domain and modern warfare. In the context of accelerating technological progress, AI is becoming a disruptive force, influencing the way armed conflicts are planned, conducted and carried out, with a major impact on global security and defence strategies.

Through a multidisciplinary approach, the study integrates concepts from technology, security and ethics to provide an overview of the benefits and risks associated with the use of AI in the military environment. It also examines how these technologies can be employed to increase the efficiency of military operations, support strategic decision-making and redefine the art of warfare in the digital era.

The methodology used includes a systematic review of specialized literature, case studies and practical examples from recent military exercises and programs, such as US Air Force projects and NATO initiatives. It enables the identification of the most effective strategies for integrating AI at the strategic, operational and tactical levels, highlighting best practices and potential vulnerabilities.

The results indicate that the implementation of AI-based technologies can lead to faster and more accurate military decisions, as well as the automation of complex processes, thereby reducing reaction time and enhancing efficiency on the battlefield. At the same time, the importance of human control and strict ethical regulation is emphasized in order to avoid the risks of abusive or uncontrolled use of autonomous systems.

Keywords: artificial intelligence; art of war; strategic, operational, and tactical level; military art; decision-making process;

INTRODUCTION

In recent years, artificial intelligence (AI) has gained an increasingly important role, experiencing exponential growth and becoming omnipresent across all areas of technology, with a major impact on the economy and on the way we live. But before anything else, we must start from a fundamental question: What is artificial intelligence, and how is it perceived in society?

Today, there is a wide variety of definitions of artificial intelligence, which differ from one to another due to the complexity of its processes and the multitude of fields in which it is applied. According to the European Council's Artificial Intelligence Act, AI is defined as *"the use of digital technology to create systems capable of performing tasks that would normally require human intervention. Artificial intelligence imitates human thinking but processes information faster and with greater accuracy"* (Artificial Intelligence Act, 2025). The Explanatory Dictionary of the Romanian Language defines artificial intelligence as *"a field of computer science that develops technical systems capable of solving complex problems related to human intelligence"* (<https://dexonline.ro/intrare/inteligen%C8%9B%C4%83/28535>).

However, the most widely accepted definition belongs to the scientist John McCarthy, who, in 1955, described artificial intelligence as follows: *"It is artificial intelligence when a machine behaves in a way that would be considered intelligent if a human were to do it"* (McCarthy, Minsky, Rochester, Shannon, 1955). Although, at first glance, the field of artificial intelligence might seem like a recent creation, the reality is quite different. The earliest research in artificial intelligence was carried out in the summer of 1956 by Ray Solomonoff, Marvin Minsky and John McCarthy during a workshop held at Dartmouth College.

In the context of accelerating technological progress, artificial intelligence has emerged as one of the most disruptive forces, influencing not only civil society but also the global security environment.

Science and warfare have always been closely interconnected, with technological innovation serving as the common element between war and civilization. Countless examples throughout history demonstrate that certain innovations have been decisive in determining the outcome of conflicts, often tipping the balance toward victory.

ARTIFICIAL INTELLIGENCE AND THE MILITARY ENVIRONMENT

The reality is that artificial intelligence is becoming one of the most important technologies of the 21st century, playing an essential role and having applications across many areas of our lives. Consequently, it has also begun to be integrated into the military domain. In this digital age, the main elements of a conflict are no longer limited to the number of soldiers or the amount of weaponry; increasingly, success depends on the use of technology to gain significant advantages over the enemy, transforming AI into a genuine force multiplier on the battlefield.

Artificial intelligence has the capacity to rapidly transform the way wars are fought, the application of tactics and techniques and the use of military technology on a global scale. The potential of AI in the military field is vast and diverse, ranging from autonomous drones and missile guidance systems to real-time decision-making and threat analysis, making it a decisive factor in modern warfare.

AI not only enhances military capabilities but fundamentally reshapes and redefines the modern battlefield, compelling combatants to adopt new tactics and continuously adapt the way they apply the principles of military art. Systems and technologies based on artificial intelligence are now at the very core of contemporary warfare, driving everything from autonomous drones to real-time battlefield analysis and ushering in a new era where speed, precision and adaptability are just as crucial as firepower.

In 2024, during an interview with *The Washington Post*, General Mark Milley, former Chairman of the US Joint Chiefs of Staff, made the following statement regarding the role of technology in modern warfare: *“The character of war, on the other hand, changes frequently. The character of war refers to tactics, techniques, procedures, doctrine, weapons, training, leader development – where you fight, when you fight: day, night, spring, summer, those kinds of things. All these details of war are what are commonly referred to as the character of war. Now, the character of war is changing, and it has changed quite frequently throughout history. One of the most common drivers of change in the character of war is technology. And I would argue that we are experiencing the most fundamental change in the character of war ever recorded in human history—again, largely driven by technology, though not exclusively by it”* (Washington Post, 2024).

Also, Geoffrey Hinton, the computer scientist often called the “godfather of artificial intelligence”, said in an interview with Katie Couric: *“The rise of killer robots will not make wars safer. It will make it easier to start conflicts by reducing*

the human and political cost of fighting. Lethal autonomous weapons – that is, weapons that decide on their own whom to kill or maim – represent a huge advantage if a wealthy country wants to invade a poor one. What prevents wealthy countries from invading poor countries are their citizens returning in body bags. If you have lethal autonomous weapons, instead of dead people coming back, you’ll have dead robots coming back” (Business Insider, August 2025).

Gradually, the battlefield tends to cede, little by little, to non-human elements. The emergence of AI-based weapons, such as autonomous drones, raises questions about preserving the human character of the battlefield in the near future, given that these weapon systems are programmed to act or react from long distances at fantastic speeds, far from human access. These trends do nothing but limit and reduce the control that humans have traditionally exercised over the conduct of war and the use of force.

The use of artificial intelligence on the battlefield – that is, systems that excel at a single task – is not a novelty in itself. What is novel is the large number and complexity of tasks that can be automated thanks to artificial intelligence. Consequently, artificial intelligence is nothing more than a tool that can be both effective and harmful to its users. For it to be useful, it requires appropriate employment and proper use within military art to be effective and efficient.

The increasing use and intensity of artificial intelligence on the battlefield creates a new concern for the armed forces employing it, namely that engagements become so fast that the human element cannot remain involved and keep up with the tempo of operations. In this context, the automation of weapon systems causes the time window available to respond to threats to become increasingly small, until the moment when only AI-equipped systems can react in time.

On the other hand, artificial intelligence will not monopolize the conduct of war. Despite its advantages, there are situations in which it is extremely limited, cannot perform every type of task and cannot be used effectively in conflict. Like any other weapon, there are countermeasures against systems that use artificial intelligence, and it would not be surprising to see them, in certain situations, turned against their users.

The ability of artificial intelligence to find its own, independent ways to solve a problem turns it into a remarkably creative tool. Devoid of human prejudices and endowed with far superior computational abilities, it brings new ways to solve problems or to suggest different solutions. Therefore, it is to be expected that the potential of artificial intelligence will be exploited by planners and decision-makers

to better understand the available options. By simulating a problem – for example in the form of a war game – and programming an AI around it, there is a very high chance of obtaining interesting and creative solutions to the problem and approaches to addressing it. In other words, it offers decision-makers additional options and a more complete overview of the decision-making process.

The use of artificial intelligence requires very specific actions and forces to define very clearly its place in the decision-making process, and to have a lucid understanding of its advantages, what its strengths are, but also its limits. Incorporating artificial intelligence into the decision-making processes of military organizations represents a clear change from previous technologies and will certainly contribute to modifying the character of war and the way military art is applied.

Artificial intelligence offers capabilities that exceed human limits in terms of speed and precision. It facilitates real-time decision-making, improves the chances of mission success, and minimizes risks to personnel. However, these advances come with certain disadvantages, including cybersecurity vulnerabilities, ethical dilemmas, and the need for new global frameworks. Understanding the role that artificial intelligence has with respect to how operations are conducted requires examining its applications and assessing the broader implications for military art.

The use of artificial intelligence in the military domain is not just a tool; it represents a change in how armed forces act. For decades, war has depended on human judgment, situational awareness and limited computing systems. Today, AI enables rapid data processing, predictive modelling, and autonomous operations, allowing forces to surpass and manoeuvre beyond traditional methodologies.

REDEFINITION OF MILITARY ART IN THE CONTEXT OF THE ARTIFICIAL INTELLIGENCE PROGRESS

Military art, in all its dimensions – tactical, operational and strategic –, is undergoing a full recalibration under the influence of emerging technologies. AI is redefining the nature of contemporary warfare, affecting both the capacity to project force and the decision-making process within the operational space and the command-and-control system. This transformation raises a fundamental question: *Does AI represent a force multiplier or a vector of vulnerability in the current military architecture?* This is the question from which we begin in developing the proposed topic.

In the digital age, artificial intelligence is redefining military art in all its dimensions – tactical, operational and strategic. These transformations are no longer

hypothetical; they have already been tested in real exercises such as the US Air Force's "*Experiment 3*" (Bussines Insider, July 2025), where AI assisted operators in targeting decisions, significantly reducing "*cognitive load*" (practicalpie.com) and confirming the value of human-machine collaboration in the *modern kill chain* (*detection, target selection, strike, assessment*) (Defense News, July 2025).

The US Air Force's (USAF) "*Experiment 3*" took place at the Shadow Operations Center Nellis (ShOC-N), within Nellis Air Force Base. It was a four-day exercise conducted by the 805th Combat Training Squadron (Shadow Operations Center–Nellis) as part of a program to evaluate and integrate artificial intelligence into the decision-making process in simulated combat situations. The aim was to accelerate and automate the kill chain decision-making process, from the tactical level to the operational level. The experiment used an AI application developed under the "*Maven Smart System*", designed to provide real-time recommendations to dynamic targeting teams. Participants compared AI-generated decisions with their own assessments to understand how the two approaches could complement each other.

The key elements of this exercise were as follows:

❖ Innovative planning and execution methodology – inspired by the "*Bamboo Eagle*" exercises. This year, the "*Bamboo Eagle 25-3*" exercise was conducted. The exercise allowed for rigorous testing of emerging technologies in a realistic simulated combat environment (AFGCS, July 2025).

❖ Involvement of manufacturers and operational observers – structured demonstrations were conducted in which ACC officials, USAFWC personnel, and other defence organizations observed the technologies in action and provided feedback for acquisition and integration processes (AFGCS, ib.).

❖ Central goal: human-machine teaming in the decision loop – AI was not intended to replace operators, but to assist them. By directly comparing AI recommendations with human decisions, the advantages of both perspectives could be highlighted. Human-generated data was also used to improve the algorithms (innovativeairforce.com, July 2025).

"*Experiment 3*" represented an important step for the USAF toward modernizing decision-making in the operational context through the integration of AI into the command-and-control chain. The focus was on:

- Rapid automation and streamlining of the decision-making process;
- Testing technologies in a realistic environment with active human participation;

- Validating concepts through feedback from real users and decision-making observers.

It is a significant step in the evolution of military doctrine toward human-machine cooperation, where AI acts as a force multiplier rather than a replacement.

1. Tactical Level: Speed, Precision, Efficiency – or Dangerous Automation

At the tactical level, artificial intelligence is being integrated into an increasing number of weapon systems, from unmanned aerial platforms (UAVs) to automatic detection and targeting systems. In conventional conflicts, AI enables real-time processing and interpretation of information coming from the battlefield, reducing reaction times and increasing lethality and precision. A tactical-level commander can benefit from algorithmically generated recommendations based on probabilistic models, which provides a significant advantage when making decisions under pressure.

However, this automation of the decision-making process introduces substantial risks. An AI system trained on incomplete or manipulable datasets can generate erroneous recommendations and the transfer of decision authority to lethal autonomous systems involves ethical, legal and operational risks. In hybrid theatres of operation, where the distinction between combatants and non-combatants is unclear, the use of AI to support tactical decisions can lead to undesirable strategic consequences, amplifying the risk of collateral damage and eroding the legitimacy of military action.

AI allows immediate reaction in dynamic scenarios, as illustrated by the Pentagon's use of Project Maven¹, capable of analysing satellite imagery and assisting in target identification with increased efficiency – the rate of target identification and designation rose from approximately 30 targets per hour (without AI) to up to 80 targets per hour (with AI).

The increase was possible because:

- Accelerated data analysis – it receives real-time data from sensors, drones, satellites and other sources, and provides suggestions for target prioritization;
- Reduced decision-making time – algorithms provide clear options, allowing operators to approve or reject the information received;

¹ *Project Maven and kill-chain targeting efficiency*, April 2025, https://en.wikipedia.org/wiki/Project_Maven, retrieved on 5 September 2025.

- Automatic filtering – AI can quickly eliminate “background noise” (irrelevant or false targets), allowing the team to focus on real targets.

The *Joint All-Domain Command and Control (JADC2)* concept connects all US military components (land, air, naval, space, cyber) into a common command- and-control system.

The integration of AI offers the following advantages:

- Optimizes the flow of information between these domains;
- Supports rapid decision-making in a data-saturated combat environment;
- Enables real-time response without the need for slow hierarchical approvals.

The following example is relevant to what was previously presented:

Total time for 80 targets:

- Without AI: 80 targets $\times$ 2 minutes/target $\approx$ 160 minutes;
- With AI: 80 targets $\times$ 45 seconds/target $\approx$ 60 minutes;

Conclusion: the same workload, completed in roughly one-third of the time.

Another relevant example is the US Army's *TITAN Project*. The first Multi-Domain Task Force (MDTF) adopts TITAN: a revolutionary artificial intelligence tool. Palantir Inc. is the primary contractor for the TITAN program, having received a contract in March 2024. The first prototype was delivered to Joint Base Lewis-McChord (JBLM) in Washington for testing in 2024 (Defense Post, August 2024).

On 18 December 2024, the First Multi-Domain Task Force (1st MDTF), a next-generation unit designed to operate across multiple domains, integrated the Tactical Information Targeting Access Node (TITAN) as a new capability, becoming the first Army unit to receive the advanced TITAN prototype.

The system was delivered to the unit in July and the Project Manager for Information Systems & Analysis (PM IS&A) completed integration, testing and operator training by December 2024, ensuring the system was fully operational.

This advanced ground-based intelligence, surveillance and reconnaissance (ISR) station is intended to revolutionize the way the Army collects, processes and disseminates critical battlefield information.

TITAN represents a significant advancement in military technology. It uses artificial intelligence and machine learning to rapidly process massive amounts of data from sensors across multiple sources, including space-based, high-altitude, aerial and terrestrial sensors. This rapid processing provides a decisive advantage over adversaries, delivering real-time intelligence and targeting information.

Key capabilities of TITAN include:

- *Rapid data processing*: TITAN's AI-based capabilities allow it to quickly analyse and interpret complex data streams, significantly reducing the time needed to identify potential threats and opportunities.
- *Enhanced situational awareness*: By fusing data from multiple sources, TITAN provides a comprehensive, up-to-date picture of the battlefield, enabling commanders to make informed decisions in dynamic environments.
- ❖ *Improved targeting accuracy*: TITAN's advanced algorithms enable precise target identification and designation, increasing the effectiveness of precision strikes.
- ❖ *Increased operational tempo*: TITAN's automation capabilities reduce the workload on soldiers, allowing them to focus on higher-level tasks and maintain a faster operational pace (army.mil, 2024).

1.1. Intelligent Technologies and Systems Implemented in Military Operations

In recent times, other intelligent technologies and systems have also been implemented, bringing major changes to the battlefield.

Use of drones and autonomous combat systems

The integration of artificial intelligence into unmanned aerial vehicles (UAVs) has raised their utility to unprecedented levels. AI-powered drones are no longer just remotely controlled devices; they are sophisticated systems capable of autonomously identifying, tracking and attacking targets. By using machine learning to analyse hours of drone footage, the workload for human analysts is reduced, while the accuracy of threat identification is increased. The development of autonomous combat systems marks a crucial moment in the evolution of warfare. These systems can identify, track and engage targets without direct human control, providing greater precision and reducing risk to military personnel.

AI-based surveillance

Artificial intelligence has revolutionized the concept of situational awareness. Surveillance systems that once relied on human observation or rudimentary sensors can now analyse patterns, detect anomalies and predict outcomes with incredible precision. A notable example is Israel's Iron Dome missile defence system, which demonstrates how AI can process data at lightning speed to calculate interception trajectories, providing real-time protection against incoming threats. Such systems exemplify how AI is transforming defence from reactive to proactive.

Threat analysis

In today's era of information velocity, AI's ability to predict and respond to threats in real time constitutes an exponential advantage. Machine learning models, trained on vast datasets, can identify cyberattacks, forecast enemy movements and deliver actionable intelligence in moments. These capabilities not only improve decision-making processes but also create opportunities to neutralize threats before they escalate into crises.

Mission planning

Operational planning is a complex process involving numerous variables and AI's role is to simplify and optimize this process through tools that use advanced algorithms to assess risks, allocate resources and generate options. By reducing human errors and accelerating decision-making, these tools increase the likelihood of mission success while conserving valuable resources.

Geospatial intelligence collection

AI's ability to process satellite imagery and drone-derived data has revolutionized data collection. AI-based software is now used to analyse geospatial data, identifying unusual activities or terrain changes within minutes instead of hours. This speed allows for more agile and informed decision-making, which is essential in scenarios where time is a decisive factor.

2. Operational Level: Information Dominance or Decision Overload

The integration of AI at the operational level has the potential to fundamentally transform the planning and conduct of military operations. In conventional warfare, AI enables the integration and analysis of large volumes of data coming from sensors, surveillance networks, and communications, generating a coherent and up-to-date common operational picture. Machine-learning algorithms can be used to anticipate enemy movements, optimize logistics and identify critical nodes in the adversary's force disposition.

In hybrid scenarios, AI becomes essential in detecting and countering information operations, influence campaigns, and coordinated cyberattacks. AI's ability to identify anomalous patterns in the digital behaviour of populations or hostile actors allows for an adaptive and multidimensional response.

However, widespread use of AI at this level can create a critical dependency on digital infrastructure, turning data networks and command-and-control systems into a vulnerable centre of gravity. In addition, the increased complexity of AI-assisted decision processes can lead to what the military literature calls "*cognitive overload*",

in which human decision-makers become prisoners of an excessive amount of information, lacking the capacity to filter the significant from the irrelevant.

AI is essential in processing large volumes of ISR data in real time. Project Maven served as a pilot project for exploiting multi-domain data, supporting the vision of network-centric warfare in the spirit of the “*system-of-systems*” doctrine and the *BMC3I* (*Battle Management, Command, Control, Communications & Intelligence*) concept (globalsecurity.org). This concept integrates the essential functions required for planning, directing, coordinating and efficiently conducting military operations. Its purpose is to provide commanders with a complete picture of the battlefield to enable rapid and accurate decision-making.

The BMC3I system aims to achieve the following: faster decision-making based on concrete data; coordination between own and allied forces; provision of a Common Operational Picture (COP); increased combat efficiency and response to threats. It can be employed in: air and missile defence systems; land, air, naval, or cyber operations; C2 centres; drone missions; NATO or multinational operations.

A BMC3I system can integrate:

- A radar that detects an enemy missile (Intelligence);
- A command centre that decides which interceptor to launch (Command);
- Encrypted communications that transmit the order (Communications);
- An operator monitoring the action in real time (Control);
- All these functions are coordinated by an integrated digital platform (Battle Management).

Some current global examples include:

- ❖ NATO AWACS (E-3A Sentry): radar aircraft providing command, control and aerial surveillance;
- ❖ ACC – Allied Command and Control Structure: NATO’s integrated command structure for coordinating multinational operations;
- ❖ Patriot System: a system operating in integration with Aegis, THAAD and other NATO platforms;
- ❖ Aegis Ashore missile defence system operated by the USA in Romania under NATO collaboration. It is part of the European Phased Adaptive Approach (EPAA) – the US strategy for missile defence in Europe.

From the perspective of emerging risk (unlikely or non-existent previously, but now relevant or critical in the present or near future), a few examples include: the use of autonomous AI in combat with lethal drones without direct human control; excessive reliance on AI for decision-making without human oversight.

The complexity of AI raises the risk of “*cognitive overload*”, where human decision-makers can be overwhelmed by the volume and weight of information. In addition, hybrid entities can launch automated disinformation campaigns using deepfakes, affecting internal cohesion and operational stability.

3. Strategic Level: Algorithmic Supremacy or Automated Escalation

At the strategic level, AI influences politico-military decision-making through its ability to analyse complex scenarios, model the evolution of conflicts and provide support in risk assessment. In conventional warfare, this capability can be used to calibrate proportional responses, identify points of geopolitical pressure, or anticipate the reactions of alliances and state actors.

In the hybrid environment, AI becomes an instrument of power projection by non-kinetic means. It can be used for campaigns of strategic destabilization, influencing public opinion, or disrupting the functioning of state institutions through sophisticated cyber operations. State and non-state actors that possess AI capabilities can build algorithmically-driven disinformation ecosystems capable of undermining social cohesion and trust in political and military leaders.

The major danger at this level stems from the opaque nature of AI – the algorithm’s “*black box*”. Strategic decisions generated by AI, without a deep understanding of how they were derived, can lead to disproportionate responses, inadvertent escalation, or errors in strategic perception. At the same time, the proliferation of AI capabilities to authoritarian regimes or insurgent groups can unbalance the international security system by democratizing access to influence and strategic sabotage technologies.

AI offers sophisticated tools for wargaming, large-scale simulations and the reduction of strategic uncertainty. Modelling nuclear effects and scenario analysis can be performed without real-world testing, contributing to planning and deterrence.

The term “*Hyperwar*” describes conflict dominated by rapid algorithmic decisions that exclude or minimize the human factor – a scenario in which strategic reactions can escalate without human discernment. Likewise, the global race for drone swarms between the USA (The New Yorker, 2023; the US Replicator, launched in 2023 by the US Department of Defense, aiming at fast, efficient production of autonomous drones) and China (mynews, 2024; researchers at Nanjing University have developed drones that can split mid-air into 2 to 6 autonomous units, inspired by the structure of a maple seed, each sub-drone having a distinct role: communications, reconnaissance and attack) – can destabilize the international

order through rapid proliferation and large-scale use.

At present, counter-technologies exist for the two programs described above, known as *anti-swarm* systems:

❖ The USA has tested anti-drone systems based on microwaves, directed-energy systems (High Power Microwave/HPM) such as THOR (Tactical High Power Operational Responder), capable of neutralizing swarms of UAVs in a single strike (airforce-technology, 2021). Operation is achieved through an instantaneous electromagnetic pulse (“*speed-of-light*”) that disables drones over a wide area.

An electromagnetic pulse weapon called “*Leonidas*” (directed-energy, High Power Microwave) (Defense News, 2023), designed and developed by the company Epirus as early as 2020 and funded under the IFPC HPM contract (2023-2024), has demonstrated the capability to disable dozens of drones simultaneously in a rapid counter-swarm demonstration. By March 2024, Epirus had delivered four prototypes of the system to the US Army.

An example of a fictional *Hyperwar* scenario would be the following: a radar detects the launch of five hypersonic missiles; AI triggers countermeasures without human approval; autonomous attack drones detect and neutralize the adversary’s command nodes; part of the conflict takes place in cyberspace, where servers, networks and satellites are disabled or compromised; critical decisions are made in less than one second, without humans understanding the full picture.

As of this date, the countries developing capabilities for *Hyperwar* are:

- USA: DARPA programs, AI systems for command and control (IDST, 2025);
- China: Massive investments in military AI, cognitive warfare, and autonomous drones (Asia Times, 2023);
- Russia: AI-integrated defence systems, automated information manipulation (cna.org, 2022);
- NATO: Initiatives to adapt to the accelerated pace of multi-domain conflict (arxiv.org, 2023).

Hyperwar is not just a possibility – it is a direction toward which modern warfare is inevitably moving, alongside technological advancement. Preparing for such a conflict involves: developing compatible technological capabilities, adapting military doctrines, and, very importantly, defining clear ethical and legal frameworks.

ETHICS, REGULATION AND HUMAN CONTROL

Strategic horizons also require a robust ethical foundation. Recent documents emphasize the necessity of FATE principles (Fairness, Accountability, Transparency, Ethics) in AI applications, along with qualities such as fairness, proportionality and decision-making responsibility.

Today, *Lethal Autonomous Weapon Systems (LAWS)* raise legal and moral dilemmas because these weapon systems are capable of selecting and engaging targets without direct human intervention, using artificial intelligence algorithms. Discussions are ongoing regarding the development of a regulatory framework for AI weapons, but no definitive outcome has been reached yet. The key question remains: *If a LAWS weapon makes a mistake, who is responsible?* The answer is uncertain: the weapon's developer, the commander of the unit operating it, or the state that owns it? The current Statute of the International Criminal Court does not explicitly cover autonomous weapons.

Within the UN, in 2014, the Group of Governmental Experts discussed regulating LAWS; however, no consensus has been reached on a prohibition. Still, several states (including the EU) call for a total ban or clear limitations.

There are also a few academic and civil initiatives, such as:

- Future of Life Institute (futureoflife.org) and Human Rights Watch² promote international treaties to ban LAWS, similar to those for anti-personnel mines or chemical weapons;
- Specialized structures (military and civilian) worldwide, along with the International Committee of the Red Cross (ICRC)³ propose a legal framework that includes: ethical and legal assessment of each system; guaranteed human control; auditability and transparency of AI decisions⁴.

LAWS raise fundamental legal and moral issues. Therefore, developing an international control framework for autonomous AI weapons is considered not only feasible but urgently necessary. Current academic discussion focuses on finding a balance between technological innovation and compliance with international norms.

The guarantee of “*Meaningful Human Control*”⁵ is a central concept in debates, meaning that any lethal decision must involve an informed and responsible human agent.

² https://www.stopkillerrobots.org/wp-content/uploads/2020/08/arms0820_web_final.pdf, retrieved on 30.08.2025.

³ <https://www.icrc.org/en/law-and-policy/legal-review-weapons/>, retrieved on 30.08.2025.

⁴ [https://undir.org/files/2021-07/UNIDIR%](https://undir.org/files/2021-07/UNIDIR%20Report%20on%20LAWS.pdf), retrieved on 30.08.2025.

⁵ https://una.org.uk/sites/default/files/2022-01/lethal_autonomous_weapons_systems.pdf, retrieved on 29.08.2025.

Returning to the context of *Hyperwar*, where AI makes rapid decisions without human intervention, FATE principles are essential, in our view, to: prevent accidents or unintended escalation; maintain human control in all situations; comply with International Humanitarian Law (IHL); preserve trust in technology and in the commanders of all structures they lead.

CONCLUSIONS

Artificial intelligence is reshaping the complexity of modern warfare, yet it cannot replace human reasoning. The success of AI implementation depends on balancing:

- Operational efficiency and cognitive peace;
- Autonomy and responsibility;
- Power projection and ethical governance.

It is imperative that military strategies incorporate robust human control, transparent policy development and international cooperation to prevent AI from becoming an agent of instability rather than a catalyst for security.

AI is both a double-edged sword and a catalyst for transforming military art. Depending on how it is integrated, regulated and used, AI can provide decisive advantages or become a major vulnerability. Military decision-makers must maintain a balance between technological innovation and human oversight to ensure national security and global stability.

AI is not only a force multiplier but also a redefiner of how military art is conceived and conducted in the 21st century. While the benefits of AI integration are undeniable, they must be weighed against the associated vulnerabilities. From operational risks posed by reliance on autonomous systems to strategic instability amplified by opaque and hard-to-control AI, the challenges are numerous.

From the perspective of military art, AI should not be viewed as a replacement for the human commander but as a sophisticated, yet imperfect, support tool. Decision-making sovereignty must remain in human hands, capable of integrating context, moral judgment and advancement wisdom – aspects that no algorithm, however advanced, can authentically substitute. Only through balanced and ethical integration of AI into military architecture can it avoid transforming from an operational asset into a systemic vulnerability.

The benefits of AI in the military context are profound and diverse. AI accelerates decision-making by processing massive amounts of data in real time, enabling military leaders to respond to threats with unmatched speed. Its accuracy minimizes

collateral damage and enhances the effectiveness of strike systems. Moreover, AI's adaptability ensures that military systems remain relevant as technologies and tactics evolve.

However, AI presents several disadvantages:

- AI systems are vulnerable to erroneous data inputs, which can lead to unintended consequences;
- Ethical concerns arise from the use of AI in warfare, particularly regarding autonomous weapons that could make life-or-death decisions without human intervention;
- Malfunctions or hacking pose serious threats – if AI systems are compromised, adversaries could manipulate military actions, resulting in catastrophic outcomes;
- Another significant issue is AI unpredictability. If a system malfunctions, it may be difficult to determine responsibility. This concern becomes more critical as technologies become increasingly autonomous. Malfunctioning AI could harm innocent civilians and accountability may be unclear.

BIBLIOGRAPHY:

1. AFGSC (July 2025), <https://www.afgsc.af.mil/News/Article-Display/Article/4284579/forging-the-fight-together-synchronizing-joint-operations-in-bamboo-eagle-25-3/>, retrieved on 1 September 2025.
2. Defense Post (August 2024), <https://thedefensepost.com/2024/08/05/us-first-titan-ground-station-prototype/>, retrieved on 3 September 2025.
3. Anneken, M. et al. (2025). *Ethical Considerations for the Military Use of Artificial Intelligence in Visual Reconnaissance*.
4. Asia Times (October 2023), <https://asiatimes.com/2023/10/us-dod-report-a-warning-of-chinas-ai-war-powers/>, retrieved on 30 August 2025.
5. Business Insider (July 2025), <https://www.businessinsider.com/air-force-tested-using-ai-make-targeting-kill-chain-faster-2025-7>, retrieved on 2 September 2025.
6. Business Insider (August 2025), <https://www.aol.com/news/godfather-ai-says-tech-making-051734216.html>, retrieved on 28 August 2025.
7. Defense News (November 2023), <https://www.defensenews.com/battlefield-tech/2023/11/01/army-gets-first-high-power-microwave-prototype-to-counter-drone-swarms/>, retrieved on 30 August 2025.
8. Defense News (July 2025), <https://www.defensenews.com/air/2025/07/22/air-force-experiments-with-using-ai-to-seek-combat-targets>, retrieved on 4 September 2025.
9. Feldman, P., Dant, A., Massey, A. (2019). *Integrating Artificial Intelligence into Weapon Systems*.

10. IDST (2025), <https://idstch.com/geopolitics/the-global-ai-arms-race-shaping-the-future-of-intelligent-warfare/>, retrieved on 30 August 2025.
11. McCarthy, J., Minsky, M. L., Rochester, N., Shannon, C.E. (1955). *A Proposal for The Dartmouth Summer Research Project on Artificial Intelligence*, <https://www-formal.stanford.edu/jmc/history/dartmouth/dartmouth.html>, retrieved on 22 August 2025.
12. NDU Press, *Artificial Intelligence on the Battlefield: Implications for Deterrence and Surprise*.
13. *Artificial Intelligence Act* (2025), <https://www.consilium.europa.eu/ro/policies/artificial-intelligence/>, retrieved on 26 August 2025.
14. Scharre, P., Lamberth, M. (2022). *Artificial Intelligence and Arms Control*.
15. Șuşnea, E., Buță, I.-C. (2021). *Artificial Intelligence in Hybrid Warfare: A Literature Review and Classification*, in Proceedings of the 17th International Scientific Conference Strategies XXI. București: U.N.Ap.
16. The New Yorker (September 2023), <https://www.newyorker.com/news/news-desk/ai-and-the-next-generation-of-drone-warfare/>, retrieved on 1 September 2025.
17. The Washington Post (2024), *Transcript: The Futurist Summit: The Age of AI: A New Era of Warfare with Gen. Mark A. Milley (US Army, Ret.)*, <https://www.washingtonpost.com/washington-post-live/2024/06/13/transcript-futurist-summit-age-ai-new-era-warfare-with-gen-mark-milley-us-army-ret/>, retrieved on 27 August 2025.
18. Yan, G. (2020). *The impact of Artificial Intelligence on hybrid warfare*, in *Small Wars&Insurgencies*.
19. airforce-technology (2021), <https://www.airforce-technology.com/projects/tactical-high-power-operational-responder-thor-drone-killer-usa/>, retrieved on 30 August 2025.
20. mynews (March 2024), <https://www.scmp.com/news/china/science/article/3255809/chinese-scientists-create-swarming-drones-can-rapidly-multiply-mid-air-create-tactical-shock/>, retrieved on 30 August 2025.
21. <https://arxiv.org/abs/1803.10664/>, retrieved on 30 August 2025.
22. <https://dexonline.ro/intrare/inteligen%C8%9B%C4%83/28535>, retrieved on 26 August 2025.
23. <https://futureoflife.org/project/autonomous-weapons-systems/>, retrieved on 30 August 2025.
24. <http://imworld.ro/2018/inteligenta-artificiala-definitie-tipuri-de-ai-cum-invata-si-ce-aplicatii-are/>, retrieved on 26 August 2025.
25. <https://innovativeairforce.com/2025/07/air-force-battle-lab-advances-the-kill-chain-with-ai-c2-innovation/>, retrieved on 4 September 2025.
26. <https://unidir.org/files/2021-07/UNIDIR%>, retrieved on 30 August 2025.
27. https://www.army.mil/article/282253/1st_multi_domain_task_force_mdtf_adopts_titan_a_game_changer_in_intelligence_and_targeting, retrieved on 3 September 2025.
28. <https://www.cna.org/analyses/2022/09/ai-autonomy-in-russia-years-reflection/>, retrieved on 30 August 2025.

29. <https://www.globalsecurity.org/space/systems/bmc3i.htm/>, retrieved on 30 August 2025.
30. <https://www.icrc.org/en/law-and-policy/legal-review-weapons/>, retrieved on 30 August 2025.
31. <https://www.practicalpie.com/cognitive-load-theory/>, retrieved on 2 September 2025.
32. https://www.stopkillerrobots.org/wp-content/uploads/2020/08/arms0820_web_final.pdf, retrieved on 30 August 2025.

STATE-OF-THE-ART TECHNOLOGIES TO BE USED IN COMMAND-AND- CONTROL SYSTEMS

Colonel Dr. Cezar POPA

– Deputy Chief, 2nd Mountain Troops Brigade “Sarmizegetusa”, Braşov -

DOI: 10.55535/RMT.2025.3.06

The use of the entire cyber, psychological and informational spectrum is specific to a conflict with variable geometry. The multidimensional operational environment is characterized by the evolution of technology, on the one hand, and by the power of information, on the other hand. It has generated strategies, operational planning processes and appropriate techniques, tactics and procedures. Technological developments have been related to all areas of PMESII. Command-and-control systems based on state-of-the-art technologies are becoming more complex and more efficient. Thanks to the integration and interconnection of new technologies within C2 systems through appropriate architectures, as well as due to the quality of human resources, command-and-control systems have exponentially multiplied capabilities in solving specific situations. Modular organization allows them to adapt, resize and develop in relation to the technological evolution and mutations produced in the physiognomy of military operations.

The architecture of a complex command-and-control system coherently and efficiently integrates sensors, decision-makers, artificial intelligence, performers (human, robotic, highly technological etc.) and support capabilities. All are interconnected (even symbiotically) in subsystems that ensure the effective planning, execution and evaluation of military actions/operations. Achieving and maintaining informational, decision-making and actional superiority throughout the spectrum of military operations, guaranteeing success at strategic, operational and tactical level, is the essential task of command-and-control systems.

Keywords: command and control; artificial intelligence; efficiency; technologies; Information Technologies;

THE IMPACT OF STATE-OF-THE-ART TECHNOLOGIES ON ACTIONS/OPERATIONS IN MULTIDIMENSIONAL CONFRONTATION ENVIRONMENTS

Analysing the impact of *state-of-the-art technologies* implemented in the architectures of command-and-control systems (C2), we consider it important to start from the fact that the current extremely complex and evolved conflict environments are characterized, in addition to technological evolution, by the power of information. Planning to achieve a common goal of the actors participating in the conflict involves exchanging information, similar working methods and joint planning sessions, which, at the strategic level prove to be often difficult. Planning in a multidimensional environment and under the conditions of the specific risks and threats of conflict with variable geometry creates challenges for both civilian and military actors. The military situation and its evolution, together with necessary information, become available in a shorter time and create the possibility of a timely response, absolutely necessary to the often-changing situations in the evolution of a modern conflict. We will briefly present some of the innovations in the field, in order to present the advantages obtained by their implementation at the level of command-and-control systems, having in mind that they have been developed at the tactical and sometimes operational level.

The *Advanced Command and Control System (AC2S)*, developed by the Czech Defence University in 2017, is a concept of how to use modern technologies to increase the efficiency of decision-making (TDDS decision-making tactical support system) and military operations/actions. In addition, the number of military personnel and their equipment for the action/operation to be conducted may also be determined in accordance with the mission requirements.

The concept of *Mosaic Warfare* has a variant of the approach, *Context-Centric C3* (Clark, Patt, Schramm, 2020). This concept assumes that during C2 processes, commanders develop a general approach to an operation that reflects their strategy and the intent of the upper echelon. The commander directs the machine-activated control system through a computer interface, assigns tasks to execute, and introduces estimates for opponents, force size, and desired effect. The machine-activated control system implements Context-Centric C3 by identifying forces (human or robotic/human, technical and weapon) that could perform the tasks

but maintains a manageable control level for the commander. The commander then decides which forces will perform the tasks. It has been driven by the idea that a modular force, capable of composing and recomposing rapidly, could offer several advantages: *Rapid incorporation of new technologies and techniques, tactics and execution procedures, high adaptability of disaggregated forces, high complexity and great difficulty for the opponent regarding the evaluation of distributed and disaggregated forces to determine the intentions and effects desired by the opponent, increased efficiency in the decision-making process, increased area of action, and implementation of an optimal operational strategy.*

Unmanned aerial vehicles (UAVs/air drones) have also experienced rapid military development. Military drones are basically the future of military technology (Eremia, 2020), which is why the list of military drone research and production companies is growing by the day. For example, Iran extensively used Shahed 129 indigenous strike drones in Syria in military operations (2016), Azerbaijan used Israeli UAVs IAI Harop in Nagorno-Karabakh, Iraq used the Chinese CH-4 drone and Turkey's Bayraktar production drones. Turkey has successfully conducted drone operations in northern Syria. The United Arab Emirates used Chinese Wing Loong II drones in Yemen and Libya in 2018. In 2019, Russia used Orion drones in Syria, and France used US drones in Mali, MQ-9 Reaper being the most visible. The Nagorno-Karabakh conflict between Azerbaijan and Armenia (2020) has best highlighted the success of drone operations. In less than 48 hours, Armenia lost 241 tanks, 4 S-300 installations, 2 SCUD installations. Moreover, 39 tanks and 24 BMP were captured. The subsequent proliferation of military air drones in general, and attack drones in particular, has made it possible for the latter to be used more and more frequently in large-scale military operations.

At this moment, we are facing the accelerated proliferation of both state and non-state military aerial drone technologies, which will generate new risks and threats to regional or global security (40 states have acquired and hold military combat or ISR drones, while 28 states are developing UAV technologies). The *"World of Drones"* American statistics place the world's states in three main groups (ib.): states that have already used combat drones in military operations, states that possess military drones but have not used them (yet) in combat and states that develop technologies for military drones.

Drone units have gained particular importance in the armed forces of state actors. Combat techniques, tactics and procedures have been adapted and folded into the capabilities of drones to provide real-time information. UAVs are used independently or in coordination with attack groups or special forces units

throughout the targeting process – target acquisition/identification, conducting fires and battle damage assessment.

A *C5I2SR command-control system* (command, control, communications, computers, cooperation, information, interoperability, surveillance, recognition) (Lehaci, 2025, p. 65), in addition to *current capabilities* (Roman, 2017, p. 56) (force command and control, common operating picture and its interpretation, information, surveillance, reconnaissance, operational and tactical planning, air situation and missile defence, joint fire and management of air, naval and land targets, effects management, manoeuvring and synchronization, information operations, force protection, resource coordination, healthcare etc.) need to expand its interoperability, macro-surveillance and recognition at least at regional level if not globally or even in space, in all environments of conflict manifestation.

It is the moment when *artificial intelligence* comes into play, which is increasingly found in the architecture of command-and-control systems. Cyber systems that will emerge from integrated approaches to all conflicting experiences over time will be able to pre-generate in advance combined evolutionary conflict schemes that can be managed before real situations degenerate.

The development of IT technologies has implicitly led to an increase in the number of cyber attacks and increased crime rates. Individuals, corporations and governments have faced extremely varied threats and cyber attacks. For example, in South Africa, crime operation run from the Deep Web segment with the Dark Web section (not accessible to the broad masses) a segment in surface Web, where normal search engines do not have access¹. In this respect, multifunctional platforms which can fight against cybercrime are needed: the detection and pro-active identification of destructive IT activities, the prevention and reduction of crime through the exchange of information and the protection of relevant users and stakeholders against emerging IT activities in the use of pro-active techniques. However, the context of technological development does not exclude the human element. It remains the most important in the decision-making process supported by an appropriate command-and-control system. Also, through the personnel who serve these technologies with their capabilities, the information becomes available to decision-makers.

¹ Proceedings of the 14th International Conference on Cyber Warfare and Security, Stellenbosch University, South Africa, 28 February-1 March 2019, platform The cybercrime combating Mapimele, Fikile V. and Mangoale, Bokang C., Council for Scientific and Industrial Research Pretoria, 0001, South Africa, e https://scholar.google.ro/scholar?q=Proceedings+of+the+14th+International+Conference+on+Cyber+Warfare+and+Security&hl=ro&as_sdt=0&as_vis=1&oi=scholar, retrieved on 12 August 2025.

Another direction in technology development are the satellites. They can be used separately in all PMESII (Political, Military, Economic, Social, Information, and Infrastructure) domains, but a group of cooperating satellites offers a wide range of advantages. Benefits include optimizing performance in mission execution and reducing or removing errors. Technically and technologically, while there are many benefits for the involvement of a large group of cooperating satellites in the command-and-control process, there are also many challenges. One of the challenges is to determine how cluster/group satellites manage to retain data on other satellites, knowledge necessary for cooperation, to respond promptly and effectively to emergencies/crisis (of any kind) and to optimise the resources needed for their efficient management. The US Air Force Space Vehicle Research Laboratory (AFRL)² has researched these challenges and many others by developing prototypes and testing them within AFRL TechSat-21 programme. In command-and-control macro-systems (developed at regional or global level by alliances), these technological components called satellites are extremely necessary because of their highly developed location and communication capabilities of any kind. Moreover, they can be even equipped with defensive or offensive combat and/or combat support systems, when space is found among the conflict environments. The command-and-control approach using satellites provides the ability to integrate traditional approaches with artificial intelligence (AI) and non-AI. Problems related to the integration (knowledge and cooperation) of many components can be solved by applying solving techniques for subcomponents (intelligent agents) and integrating individual solutions to reach a final, complete solution.

With regard to the concept of space warfare (ground-space operations – *ground attack of satellites*, space-space operations – *satellites attack satellites*, space-ground operations – *attack executed by satellites on ground* and combined devices), our opinion is that, considering it a *symbiosis of architectures* of the ground-based and satellite control systems, in conjunction with the control part of the execution of military or non-military operations by disaggregated forces, the concept of *mosaic warfare* may be the optimal solution for models of command-and-control systems extended at strategic level, with the possibility of rapid adaptation to the changing geometry of latest conflicts.

Any nation with space intelligence gathering capabilities has also the possibility of optimal use of its high-performance ground attack installations (high-precision

² "TechSat 21: Advanced Research and Technology Enabling Distributed Satellite Systems", Overview Briefing of TechSat 21, <http://www.vs.afrl.af.mil/vsd/techsat21>, retrieved on 18 August 2025.

striking systems) and vice versa. Thus, the best-performing missiles become somewhat useless without observation and information from space.

Specifically, the results obtained in identifying the *impact of state-of-the-art technologies and artificial intelligence* on operations conducted in the *multidimensional conflict environment* will be presented through a brief SWOT analysis.

A. STRENGTHS	B. WEAKNESSES
Developing the efficiency of decision-making process: - rapid (real-time) transfer of information; - rapid, comprehensive, synthetic, analytical and objective analysis of specific situations in the field/area/region; - automatic generation of COAs based on big-data access and analysis algorithms used by artificial intelligence embedded within C2; - quick force taskorg set up, in accordance with the mission requirements (number of military and equipment) necessary to carry out the action/operation; - optimising/updating the organisation of military systems as well as doctrines, primarily by changing the ratio of human resources and materials/equipment involved; - The concentration of human resources will be on the really relevant/important/critical aspects; Development of response force capabilities: - Leads to increased speed of military operations: 1. The huge amount of data available may increase the speed of decision-making, but if the decision-making process is overwhelmed with data/information, it may decrease the speed of this process in the absence of adequate management tools.	- Partial replacement of the human factor in the decision-making process/how far certain tasks should be delegated to the AI (e.g. during the Cuban missile crisis, human decision-makers changed their minds about actions/attacks. AI would not have done so in the absence of actual data to generate this change); - Possibility of decreasing or losing human control in the execution of missions using robotic weapon systems; - The need for exponential growth of measures to protect information and artificial intelligence systems; - COAs generated by artificial intelligence lose sight of military art elements, data and information analysis being algorithmic, and may be overlooked essential human-specific analytical variables; - Involves the error-free use and/or integration of automated platforms – robots, drones etc.; - Creates problems related to moral/ethical aspects as well as those concerning the legality of the use and actions of Artificial Intelligence; (not yet really debated/profound discussions on moral issues; morality and legality are determined by the power brokers/those who make the laws/leaders);

2. Increases process's speed and boosts decision-making process; 3. Increases the quantity and quality of processed information and products/ processes, as well as the efficiency of processes /activities; 4. Significantly/decisively contributes to increasing the level of understanding of the data provided by the multitude of sensors. - disaggregated force (capable of composing and recomposing rapidly adapted to the specifics of the mission); - reducing human losses by using advanced (robotic, automated) combat technologies; - ergonomics in the use of forces and equipment by performing large-scale operations or surgical blows, as needed. Communications: - communications and portable technologies that communicate within networks at soldier level; - different networks communicate with each other, - facilitating the creation of tactical, operational, strategic information networks; Issues relevant to Command Points within C2: <i>CP mobility</i> is increased by using modular (container) infrastructure and mobile networks are built up based on miniaturisation of components and terminals, for use in heavy humidity conditions etc. <i>Secure wireless.</i> Currently, secure IP-based transmissions can only be made from static locations, but state-of-the-art technology will allow mobility.	- Developing AI is a task in itself; - AI is a real challenge – training an AI is done through real processes and activities, not simulated, such as training in a military range. E.g.: in 2003 a Patriot system operating on automatic operating mode shot down a RAF (UK) aircraft, and a few months later, in another similar incident, a USAF aircraft was shot down; Communications: It is necessary to secure portable devices for use in military networks (military personnel do not have individual secure tactical terminals); increase in the need for IT specialists; processing speed and storage capacity are critical as the amount of data increases exponentially and the human factor cannot process them;

<i>Cyber Security</i> – physical destruction can be caused by IT means (e.g. Stuxnet – destruction of Iranian centrifuges); use of troll factories in shaping public/social agendas and opinions at the level of a society (e.g. fakenews phenomenon, Russian troll factories). <i>IT/network access</i> – building the common operating picture, access and processing of signals and images/maps, ISR integration systems, security etc.; (one possibility is to access information stored in cloud – see US government contracts with IT giants for cloud capabilities). Low-altitude satellite networks and other civilian infrastructures can be used for military action by encrypting signals and data, as they make it impossible to completely destroy the system/multiple redundancy (similar to the STAR system).	
B. OPPORTUNITIES On the efficiency of the decision-making process: - instant access to specially designated or international databases, information; - extremely fast processing of data and information (with an immeasurably higher speed than the possibilities of the human brain); - the connection and interconnection of command-and-control systems in extensive multinational operations; - the use of C2 modules in a rubic or mosaic mode (as a whole or in combination, according to the specifics of the operation and at the required level); - architectural flexibility of the platforms used and C2 modules;	D. THREATS - the real factor of the databases used, - neutralising C2 systems or intelligent weapons systems through imminent cyber attacks; - the great influence of artificial intelligence on human decision-making (decision based on experience, knowledge and talent can be overlooked); - taking control of weapon systems by artificial intelligence or the enemy through cyber attacks on the infrastructure of poorly protected C2 systems; On communications: - Connectivity and traffic levels raise access/risk/vulnerabilities issues;

- simultaneous action with the response cells actions planning; - can contribute to the construction/validation/verification of a context, a reality, in the military field of the Common Operating Picture/Situation Awareness. - immense power in identifying and classifying various objects/equipment/threats/individuals, with an incomparable precision and speed higher than man. - Building relevant databases can facilitate the success of military operations 1. Example: based on databases with images of enemy equipment, a vector can prioritize its first attacks, in which impact zone can cause the most damage, make difference between friend or foe etc.; 2. Large enough biometric databases allow for the construction of diagrams/networks and the extremely rapid identification of critical elements/objectives in a human network – see Baghdad in the Gulf War, Afghanistan, criminal databases... 3. Increased accuracy leads to a decrease in the likelihood of a misperception/mistake and an escalation of the security situation can thus be avoided. On the disaggregated, technological and robotic force: - Rapid implementation of new technologies and techniques, tactics and execution procedures; - High adaptability of disaggregated forces; - Complexity and great difficulty for the opponent regarding the evaluation of distributed and disaggregated forces to determine the true intentions and opponent's desired effects;	- The Internet of Things will generate huge amounts of data and metadata, and its control and access may be restricted or may generate disputes. E.g.: Some companies may be restricted from entering the market; - Access to metadata can provide relevant data and if pieced together can lead to critical information. E.g.: Cambridge Analytica scandal – Brexit, US election; - Modelling/influence the public opinion/a critical mass to have a desired reaction (action or passivity). E.g.: elections won at thresholds below 5%, by presenting a small number of voters/electoral passivity. E.g.: Sun Tzu – <i>“win a war without waging it”</i>.

-Increased efficiency in decision-making process during the execution of the mission; - Increase in the area of operations by ergonomic use of force; - Optimal operational strategies – exponential reduction of resource losses of any kind; - By increasing the degree of automation, more robotic equipment will be integrated at the tactical level, while the human resource will be more engaged in the analysis and decision-making process.	

**TECH INTEGRATION WITHIN THE MODULAR AND FLEXIBLE
COMMAND-AND-CONTROL SYSTEMS**

Integrated systemic approaches into the art of operational planning capture the fact that up-to-date technologies ensure information flows at all levels (strategic, operational and tactical).

The starting point for optimizing conflict with variable geometry command- and-control systems is that they *must extend* their interoperability, macro-surveillance and recognition capabilities.

The equipment used is based on the latest technological discoveries and developments. For example, Network Enabled Ability (NEC), a term used at NATO level for the system designed to achieve greater military effect through integrated use of information systems, integrates all the equipment and technology. Artificial intelligence is increasingly integrated into highly complex IT systems that are able to learn for themselves from situations that are managed with their help. Researches in this field have developed artificial intelligences to work on the same principle as the human brain. They can analyse algorithmically and synthetically, and can generate quick solutions that are absolutely necessary in time sensitive situations in the decision-making process. The commander may be offered, in a relatively short time, already analysed COAs, using variables that were previously fed to the system, and using a comprehensive database. The decision will be made much faster, whether a system-generated course of action or an intuitive or a combined course of action is taken. However, the human factor plays the most important role.

The *integration and interconnection of subsystems and technologies* necessary for the operation of command and control is important in the decision-making process. Identifying and/or constructing tools to analyse the operational environment and to identify the procedures for action necessary for command-control, under the conditions of managing conflict-specific situations with variable geometry becomes imperative.

The *process of making forward-looking and correct decisions* in these situations is conditional on adapting military action to real strategic situations and addressing all areas of conflict with variable geometry in planning and leadership. In this respect, the modularity of the command-and-control systems will lead to increased structural and actional mobility. The use of high-performance technologies will lead to a significant increase in decision-making and action capacity on: increasing the distance of action and precision that will make it possible to selectively and punctually engage objectives; the ability to choose the target effect from a wide range of non-lethal and lethal effects, which will give the military decision greater flexibility; achieving the state of confusion necessary to obtain surprise and victory through processes of psychological, information warfare and misleading operations; increase responsiveness, optimizing management and achieving the viability of technical systems.

The result of the use of high-performance technologies, their *integration and interconnection of the subsystems at C2 level* will result in: significant increases in the mobility of systems and subsystems and decision-making capacity; increasing the potential of forward-looking; broadening the range of planned and conducted operations; diversification of decision-making and management procedures and management of military or non-military actions/operations; solutions for multidimensional protection of forces/objectives.

THE ROLE OF INFORMATION TECHNOLOGIES AND ARTIFICIAL INTELLIGENCE IN OPTIMISING DECISION PROCESS

Information technologies developed to date in the military ensure information flows within the forces command and control, obtaining the Common Operating Picture and its interpretation, in the field of intelligence, surveillance, reconnaissance, strategic, operational and tactical planning, air situation and missile defence, joint fires and management of air, naval and land targets, effect management, manoeuvring and synchronization, information operations, force protection, coordination of resources, healthcare etc.

In the face of the risks and threats of a conflict with variable geometry (Mitulețu, 2019), real-time communication between national or multinational forces, command and support structures, as well as between strategic leadership elements or other elements with security and defence responsibilities is a determining condition in achieving the desired effects throughout the execution of non-military or military operations. Information and communication technology have the lead position, both in terms of the number of innovations and their impact in the military field. At the command-and-control level, regardless of the structure, field or level at which it is conducted, cognitive systems will construct *scenarios based on relevant assumptions and contextual data*, offering decision-makers alternatives/COAs or, in certain situations, making their own decisions with direct impact on operations. This effect of the sharing data and information by computers and people is of most importance in the decision-making process. The next level is to *model data and information* and classify them semantically to *reconstruct virtual possible scenarios from reality*. It is the level to which all command-and-control systems used in the effective management of latest crises and conflicts tend, particularly of those whose geometry is constantly changing.

Information technology is defining, but the human element gives it the shape we perceive. Digital development and new information technologies have led to significant changes in the preparation and use of the human resource involved in both decision-making (architecture, structures and infrastructure) and execution (technical and equipment, combat and armaments). The global military trend is to transform C2 architectures and models folded into the current requirements generated by the variable geometry conflict using the effects generated by new information technologies based on digital evolution. Artificial intelligence implemented in command-and-control systems will anticipate human intentions and provide options/variants/scenarios/COAs before we actually need them.

In the military field, information is managed by intelligence structures/units (Intelligence-INTEL). The role of INTEL units is to provide decision-makers with a complete picture of actors participating in the conflict and the conflict environment (or the operational environment – in a narrower understanding of the conflict environment). This image should include the actors' status (temporary objectives, strategy, doctrine, tactics, composition, capabilities, gravity centres, vulnerabilities, capabilities and intentions). INTEL must provide a complete picture on the enemy, its culture, traditions and history, shaping its societal and ethnic environment. An information process carried out in support of the decision-making process must be timely, sound and accurate. It is based on the need for the rapid information

flow from all sources available through state-of-the-art information technologies. The information shall be collected on the basis of the Commander Critical Information Requirement (CCIR) after it has been previously identified.

An information cycle comprises four stages – planning, collection, processing and dissemination of the final product, and information technologies are undoubtedly the component that ensures the accuracy and speed of the process and implicitly of the information cycle. The information thus processed ensures the Comprehensive Picture of the Operational Environment (CPOE) in terms of the development of the main characteristics of the operational environment (terrestrial, maritime and air) as well as of the political, military, economic, social, infrastructure and information fields of opponents, allies and neutral actors that may influence operations of any kind.

The complex and continuous process of planning, coordination, synchronization and conducting information activities in order to achieve the desired effects on the ability of understanding and perception, the will and capabilities of the opponent or other entities, in support of the achievement of military objectives, while at the same time ensuring the protection of their own is also supported and is based on state-of-the-art and ever-improving information technologies. This process consists of performing information operations (Info Ops).

Advanced information technologies are used in shaping operations, focused on changing or strengthening the perceptions and attitudes of the opponent or potential opponent, or in information protection activities, focused on maintaining freedom of manoeuvre in the information space by defending the data and information that support the decision-making process. There are also attacks on data and information systems that support the opponent or potential opponent and on those information systems, surveillance and target acquisition systems (Intelligence, Surveillance, Target Acquisition and Reconnaissance/ISTAR) that use information to support the decision-making process.

Information technology generates developed capabilities, tools and techniques or key elements specialized in information activities. For example, information technology helps PSYOPS (different from public information) to have direct control over the content, dissemination and audience to achieve objectives of supporting the general interests of force, weakening the combative will of opponents or potential hostile target audiences, strengthening the beliefs of friendly or allied target audiences, attracting support and cooperation of neutral and undecided, supporting reconciliation and tolerance actions, promoting a positive

image of military forces deployed in the theatre of operations and countering hostile psychological actions.

Operation security requires identifying and protecting critical information considered Essential Elements of Friendly Information (EEFI) and can only be achieved through state-of-the-art information technology. Information security ensures the confidentiality, integrity and accessibility of information through procedural, technical and administrative control based on unbeatable information technology.

Misleading the opponent is achieved by manipulating, distorting and falsifying information and applying both informational and traditional means and techniques and technologies.

Electronic Warfare (EW) supports Info Ops by using advanced technologies so that critical information underlying the opponent's decisions and the systems that carry this information is affected. Commanders can use EW activities in the context of influence measures, and prevent the opponent from exploiting these opportunities.

Information technology also supports the engagement of key leaders by facilitating bilateral discussions between commanders and their military and civilian correspondents at the same level of influence, speaking on various occasions, in the presence of the media and/or key decision-makers, in the preparation and dissemination of interviews, for a particular media segment, with broad coverage and a great influence on the targeted objectives, conferences prepared to address specific topics of interest, with potential for influence.

The opportunity and efficiency of computer network operations (CNO) depend on the degree of dependence of the opponent on the information technology used. It materializes through executed attacks on the opponent's computer networks and the defence of their own networks. Attacks are carried out by feeding flawed codes (computer viruses) and manipulating data for the purpose of modifying the characteristics and performance of devices or of disclosing the information contained therein by exploiting them. Maintaining the capabilities that support the decision-making process is essential for the execution of operations. A procedure is therefore being developed for maintaining a defensive attitude and using protective techniques to monitor and penetrate information systems also on the basis of existing and permanently developed information technologies. The aim is to identify and define the type of attack and to have an appropriate response through actions to limit/delay and/or wind up their effects.

The challenges of artificial intelligence in the field of security and defence are not few and must be taken into account for current conflicts with variable geometry or for future ones. On this date we are witnessing a major advance in the use of AI in all areas of life, this type of technology providing a more comfortable life for those who use it. But AI has also a strong negative social impact by reducing personal privacy and can lead to a climate of insecurity if not properly managed. Moreover, AI has the ability to self-learn. It contributes to the *redefinition of both the security and defence concept, and strategy and the operational planning process* where planning for a potential conflict campaign/operation is required. In this respect, the command and control structures at the strategic, operational and tactical level need to develop capabilities to anticipate potential attacks on national or regional security (in the context of a regional, multinational, extended conflict) and on the security of forces in the area of operations (for operational-tactical level).

AI can have beneficial effects (efficiency of decision, protection of force, reduction in the number of human victims etc.) but also destructive ones (in the field of security, the future of humanity) (Ene, 2019). This technology poses a major challenge for command-and-control systems and beyond. It is absolutely necessary in the conditions and situations created during conflicts with variable geometry for timely management through analysis and informational synthesis of the rapid change in the geometry of conducted operations or even of conflict in general. At the moment, we consider that it is irreplaceable in the architecture supporting national, regional, global or even space defence and security. The fight goes for supremacy in the field of information technology and artificial intelligence in order to have global control. However, the implementation of AI in *command-and-control systems* and *weapon systems* without clearly drawing its limitations in decision and control and without maintaining absolute control by the human factor over it can have a destructive effect. The questions that need a quick answer are those related to how far should certain tasks be delegated to AI. For example, during the Cuban missile crisis, human decision-makers changed their minds about actions/attacks. AI would not have done that in the absence of real data to generate that change. Another question that arises is about moral/ethical issues as well as concerning the legality of the use and actions of artificial intelligence (Development of AI is a task in itself and has not yet been actually debated/deep discussions on moral issues). A weapon system using artificial intelligence is initially programmed (target determination and destruction) and later it will schedule itself on the basis of AI. How will we control these completely independent weapons? When and if an autonomous system kills, who is responsible for that action? (forbes.com, 2019).

We all know that a soldier's mission is particularly dangerous, but certain missions that soldiers must carry out are extremely difficult, if we are talking about clearing a building where enemies are found or deactivating a bomb. What if we had the ability to send robots to carry out such missions instead of humans? If something did not go according to plan, we would just lose material resources. We see important benefits of this technology, but can we be sure that this approach will not completely change our way of life? A real challenge is to train an AI through real processes and activities, not simulated, such as training soldiers in a range. For example, in 2003 a Patriot system operating on automatic operating mode shot down a RAF (UK) aircraft, and a few months later, in another similar incident, a USAF aircraft was shot down. The US successfully uses unmanned aircraft that carry out surveillance missions and can launch missiles at targets (science.howstuffworks.com). The effectiveness is undeniable but there is controversy over the morality of these actions. While the drones are doing their job at a height, the enemy has absolutely no chance of defence (The Nagorno-Karabakh conflict of September 2020 – Armenian losses: destroyed 241 tanks, 4xS-300, 2xSCUD and captured 39 tanks and 24 BMP all within 48 hours since the outbreak of the conflict and all as a result of drone action. Azeri losses – unspecified). In this scenario, a human operator will decide when that drone will open fire. The use of weapon systems or autonomous weapons requires a thorough risk analysis, as technology can quickly replace the human factor due to information processing speed and algorithmic decision-making speed.

In conclusion, command and control should not be delegated from the human factor to AI. It is necessary for the human factor to have control over AI and command-control over disaggregated forces with rapid aggregation capability, fully or partially robotic.

CONCLUSIONS

The evolution of artificial intelligence and information technology in recent years is significant and unavoidable. Today, we are no longer talking about computers that are capable of generating solutions, following pre-defined algorithms, but we are talking about computers and devices that have the ability to develop their own learning capacity. With reference to the security and defence subjects and applicability in the military field, we consider that new information technologies in conjunction with AI will develop the *decision-making process* specific to operational planning developed using complex and modular command-and-control systems at all hierarchical levels. AI terminals will be found in all automated, robotic weapon

systems within the disaggregated forces (with the possibility of rapid aggregation on the specifics of the mission to be executed) reducing the risk of human losses, increasing the level of force protection, increasing reaction speed and firepower etc. Artificial intelligence has a potential role to play in reducing the use of human resources in various fields, processes or activities, but it requires the use and/or integration of digital, automated platforms as well as robots, drones etc.

In the sphere of communications, technology is evolving rapidly, the trend being to have communications and portable technologies that communicate within networks from the military structure level to the individual level. It is preferable to have the possibility that different networks (belonging to or serving different structures) to be able to communicate with each other (tactical, operational, strategic). This level of connectivity and traffic (e.g. 5G) can, however, raise access issues, create risks and generate vulnerabilities. Building the Common Operating Picture requires access and processing of signals and images/maps, ISR integration systems, security etc. AI can have quick access to information stored in cloud (see US government contracts with IT giants for cloud capabilities). For the human factor, the processing speed and storage capacity *are critical* as the amount of data increases exponentially and the human factor cannot process and store them. From this point of view, it is recommended to implement AI at the level of processing data stored in macro-exponentially growing databases.

Low-altitude satellite networks and other civilian infrastructures can be used for military action by encrypting signals and data, as they make it impossible to completely destroy the system with multiple redundancy (similar to our STAR system).

Therefore, *the impact of the state-of-the-art technologies implemented in C2 systems is manifested concretely in terms of data traffic, accurate analysis of information and its dissemination, efficiency of decision-making and optimising³ and achievement of common objectives for actors participating in the conflict⁴.*

BIBLIOGRAPHY:

1. Clark, B., Patt, D., Schramm, H. (2020). *Mosaic warfare exploiting artificial intelligence and autonomous system to implement decision – center operations*, Center for Strategic and Budgetary Assessments, <https://csbaonline.org/research/publications/mosaic-warfare-exploiting-artificial-intelligence-and-autonomous-systems-to-implement-decision-centric-operations>, retrieved on 10 August 2025.

³ By implementing AI in information systems and facilitating AI access to big data databases, thus generating algorithmically-based comparative analyses, rapid and with results that materialize in generating concrete and coherent courses of action as well as in establishing taskorgs by type of mission.

⁴ Through rapid exchange of information, similar working methods and availability for joint planning sessions.

2. Ene, P.-V. (2019). *Beneficii și riscuri în domeniul inteligenței artificiale*, Conferința științifică internațională Gândirea militară românească, București.
3. Eremia, C. (2020). *Epoca războaielor dronelor aeriene s-a instalat definitiv?*, <https://monitorulapararii.ro/epoca-razboaielei-dronelor-aeriene-s-a-instalat-definitiv-1-31794>, retrieved on 22 August 2025.
4. Hariuc, N. (2019). *Spațiul, un nou câmp de luptă*, <https://www.rumaniamilitary.ro/spatiul-un-nou-camp-de-lupta>, retrieved on 17 August 2025.
5. Lawrence, F. (2019). *Viitorul războiului, o istorie*, translated by Corina Hădăreanu. București: Editura Litera.
6. Lehați, N.-T. (2015). *Tendențe în evoluția sistemului de comandă și control la nivel operativ*. București: Editura Universității Naționale de Apărare "Carol I".
7. Mitulețu, I. (2019). *Siria – spațiul unui conflict cu geometrie variabilă și consecințe imprevizibile*, in *Revista Academiei de Științe ale Securității Naționale*, no. 1.
8. Proceedings of the 14th International Conference on Cyber Warfare and Security, Stellenbosch University, South Africa, 28 February-1 March 2019, platform The cybercrime combating Mapimele, Fikile V. and Mangoale, Bokang C. Council for Scientific and Industrial Research Pretoria, 0001, South Africa, https://scholar.google.ro/scholar?q=Proceedings+of+the+14th+International+Conference+on+Cyber+Warfare+and+Security&hl=ro&as_sdt=0&as_vis=1&oi=scholar, retrieved on 12 August 2025.
9. Roja, Al. (2018). *Transformarea digitală – provocare, risc sau oportunitate?*, *Research and Education*, no. 2, www.researchandeducation.ro, retrieved on 22 August 2025.
10. Roman, D. (2017). *Abordări sistemice integrate în arta planificării operaționale*. București: Editura Universității Naționale de Apărare "Carol I".
11. "TechSat 21: Advanced Research and Technology Enabling Distributed Satellite Systems", Overview Briefing of TechSat 21, <http://www.vs.af.mil/vsd/techsat21>, retrieved on 18 August 2025.
12. <http://economie.hotnews.ro/stiri-it-12494265-kaspersky-exista-dovezi-solide-sunt-legaturi-stranse-intre-armele-cibernetice-stuxnet-flame.htm>, retrieved on 13 August 2025.
13. <https://science.howstuffworks.com/robots-replacing-soldiers1.htm>, retrieved on 22 August 2025.
14. <http://windows.microsoft.com/ro-ro/windows/viruses-faq#1TC=windows-7>, retrieved on 22 August 2025.
15. <https://www.darpa.mil/news-events/>, retrieved on 12 August 2025.
16. <https://www.dw.com/ro/irakul-ringul-de-lupt%C4%83-american-iranian/a-51853825>, retrieved on 13 August 2025.
17. <https://www.forbes.com/sites/cognitiveworld/2019/01/14/the-weaponization-of-artificial-intelligence/#4877c3723686>, retrieved on 22 August 2025.
18. <http://www.vs.af.mil/vsd/techsat21>, retrieved on 22 August 2025.

RUSSIA'S HOBBSIAN WAR AND UKRAINE'S KANTIAN IDEA OF UNIVERSAL PEACE – ONTOLOGICAL APPROACHES TO THE CONTEMPORARY EASTERN EUROPEAN WAR PARADIGM FROM AN ANTHROPOLOGICAL PERSPECTIVE –

Sergeant Traian OSTAHE, Doctoral student

811th Infantry Battalion "Dej"

DOI: 10.55535/RMT.2025.3.07

In this scientific endeavour, we propose as the main research objective the examination of the ideological component of the Ukrainian-Russian conflict, analyzed from the perspective of the two great philosophers of Western science and culture – Thomas Hobbes and Immanuel Kant, as well as their significant integration into the current context of the Russian-Ukrainian war. Such an approach can serve as a working tool that will lead to a better understanding of the conflict and a necessary perspective for planning military operations, but also for managing post-conflict operations.

By engaging with these philosophical frameworks, the study aims to uncover the underlying moral and political principles that influence decision-making processes at both strategic and operational levels, thereby contributing to more comprehensive conflict resolution strategies.

Keywords: Ukrainian-Russian conflict; Thomas Hobbes; Immanuel Kant; political sciences; Eastern Europe;

Editor's note: The English quotations were drawn from the public-domain electronic editions available at Luminarium (Renaissance Editions), based on the University of Adelaide mirror of the ERIS Project text (<https://www.luminarium.org/renaissance-editions/hobbes/leviathan.html>), and at the International Relations and Security Network, (<https://www.files.ethz.ch/isn/125464/605.pdf>).

PROLEGOMENA

The period immediately following the Cold War, instead of leading to a new era of order and stability in international relations, witnessed a series of violent outbreaks and growing instability, especially in developing countries. Much has changed globally in the two decades since 1989, but the main issues that define relations between people and between people and states have remained largely the same.

Political thinking and decision-making are inspired by the political, economic and social context in which it develops, meaning the malleability and adaptability of intentions depending on independent factors; this does not apply to Russia, for example, where, for centuries, they have been marching on a conception similar to Lucius Accius' thought: *"let them hate me, but fear me"* (dictionar-citate.blogspot.com, 2011).

In the present scientific endeavour, we propose as our main research objective the ideological component of the Russian-Ukrainian conflict analysed from the perspective of two great philosophers of Western science and culture. We are considering the study of the representative ideas of the two great scholastics, Thomas Hobbes and Immanuel Kant, as well as their significant integration into the current context of the Russian-Ukrainian war. Such an approach can constitute a working tool at the disposal of the intelligence analyst and commanders, a tool that leads to a better understanding of the conflict and allows for the achievement of a forecast and a perspective necessary for the planning of military operations, but also for the management of post-conflict operations.

The scientific research methods used were observation, analysis and case study, having an inter- and transdisciplinary character, carried out through investigation, interpretation and rational study of the results obtained by prestigious researchers from various disciplines, such as military sciences, philosophy, political sciences, psychology, sociology, social psychology, cultural anthropology, management of strategic, operational and tactical analysis and planning.

We believe that an analytical approach to the ideological spectrum of the conflict space in the context of culture and the laws that govern mass movements can lead to the understanding of crises and conflicts, resulting in both their anticipation and the influence and shaping of the environment and the collective mentality residing in that space.

Also, this type of approach can contribute to the success of operations, by reducing risks and exploiting opportunities, due to the possibility of influencing collective behaviours and perceptions early on. Thus, in order to respond to what people think collectively, in the conflict space, it will be necessary to identify how they develop cognitive activities that can lead to the crystallisation of the laws of thought in their dynamics. By understanding these, we can anticipate reactions in different contexts, which can lead to the creation of a perspective, in the sense of knowing what are the motives based on which certain events occur with the possibility of generating the most appropriate responses to the newly created situation. In addition, this type of approach could improve leadership and planning capacity not only at the operational and tactical level, but also at the strategic level.

THE RUSSIAN-UKRAINIAN WAR EVENT ANALYZED THROUGH HOBBSIAN PERSPECTIVE

Thomas Hobbes places three causes at the root of interhuman conflicts: rivalry, distrust and the desire for glory. All of these are fed by the lack of resources and cohesion between people. In Hobbes's view, persons invested with absolute power should exercise that authority only for the purpose of peace and defence, essential characteristics for supporting the state of well-being and prosperity that every citizen needs. All those leaders who pursue goals that do not have peace and defence in mind will never manage to maintain their received authority.

Even though, in the first years after the collapse of the USSR, the Russian Federation was weakened and strongly affected by the new international realities and could not cope militarily and politically with NATO expansion, it nevertheless tried to limit the presence and influence of the US in Europe by creating a buffer zone, that is, the space of former Eastern Europe. Simultaneously, it initiated an aggressive lobby against NATO expansion, by all possible diplomatic means. *"Historically, Russia's geographical vulnerability has made establishing buffer zones critical to national security. Erosion of the buffer, as in NATO expansion eastward, is viewed by the Kremlin as a threat to vital security interests and may result in attempts to reestablish a more secure perimeter (as in Ukraine)"* (Ziegler, 2020-2021).

The Kremlin's interventions in international conflicts can also be interpreted and analyzed from the somewhat surprising perspective of cultural diplomacy by exercising Russia's influence in the ex-Soviet space, especially since this geographical area represented the foundation of the grandeur and hegemonic ambitions of Russian leaders. However, as Professor de Tinguy argues, the erosion of Russian positions is also cultural. The affirmation of identity encompasses all new states through the promotion of national culture and through historiographical revisions, symbols of independence and rupture with the past (de Tinguy, 2008, pp. 42-43).

From a Hobbesian perspective, approaching the issue in the sense anthropologically, Russia can be defined as a “...mortal God...” and “...an artificial man, though of a greater stature and strength than the natural, for whose protection and defense it was intended...” (Hobbes, 2023, pp. 5, 134).

Continuing the Hobbesian perspective, Russia, through the actions carried out against Ukraine, would aim to transform Ukraine into a civil community, which in Hobbesian language can be translated as the place “...where sovereign power is acquired by force (...) when many together, for fear of death or bonds do authorise all the actions of that man or assembly, that hath their lives and liberty in his power...” (ibid., XX, *Despre dominația paternă și cea despotică/Of Domination Paternal and Despotical*, art. 1, p. 155¹).

The ability to be a good connoisseur of war events can also be proven by the fact that, several centuries earlier, Hobbes described the context in which social disorder and chaos can arise: “For those men that are so remissly governed that they dare take up arms to defend or introduce an opinion are still in war; and their condition, not peace, but only of cessation of arms for fear of one another; and they live, as it were, in the procincts of battle continually” (ibid., XVIII, *Despre drepturile suveranilor prin instituire/Of the Rights of Sovereigns by Institution*, art. 9, p. 141). The state of affairs described by Hobbes can be easily observed even by individuals less familiar with the principles of *ars bellum* within the current context of the situation in Russia.

If, in certain circles, the invasion of Ukraine by Russia has received a certain validation and, from the point of view of some, acquires a certain solidity, we propose for analysis Hobbes’s opinion on the concept of justice: “...As I have heard some say that justice is but a word, without substance; and that whatsoever a man can by force or art acquire to himself (...) is his own, which I have already shown to be false (...) Wherein they argue as ill, as if the savage people of America should deny there were any grounds of principles of reason so to build a house as to last as long as the materials, because they never yet saw any so well built... excepting by external violence” (ibid., *Despre funcția reprezentantului suveran/On the Office of the Sovereign Representative*, art. 5, p. 259).

The analysis of the conflict in Ukraine from a Hobbesian perspective could continue, but for reasons of space, we stop here. Hobbes’s objective regarding violence and war is assumed, which can be proven by his own words: “And such are those which I I have in this discourse set forth: which, whether they come not into the sight of those that have power to make use of them, or be neglected by them or not”

¹ To clarify, in Chapter XVIII – Of the Rights of Sovereigns by Institution, Hobbes develops extensively about the civil community, but he does not conceptually define the civil community, but only reiterates what was known at that time about the paradigm of the reality of a civil community (author’s note).

(ibid.). Through this quote, we can realize that he did not write the famous treatise to gain any material or other benefits from any power contemporary worldly and certainly not to win the sympathy of his followers. At the same time, he still hopes for some understanding for those in power, in order to be able to participate in the effort to change things in the world.

KANTIAN PERCEPTION OF PEACE

The paradigm of democracy claims that democratic states do not have conflicts. According to this theory, a Europe of democratic regimes, which share common ideals and values, such as respect for fundamental human rights and freedoms, the rule of law, freedom of the press etc., is a Europe in which there are no conflicts. However, reality proposes an antinomic perspective. Within the European space, there are democratic states that are still facing this problem. The European Union is trying to promote democracy, with the aim of creating a security zone that goes beyond the European space.

The ideological orientation of Ukrainians began to manifest itself with the dismemberment of the USSR, which gave Ukraine the opportunity to act according to its own desires, at least apparently, but the division of the population between East and West influenced the political leadership in Kiev to often oscillate between the West and the East (Brookings, 2015).

From a geopolitical perspective, the involvement of the Russian Federation and USA in supporting candidates in the 2004 and 2010 presidential elections transformed the vote of the Ukrainian population into a geostrategic option for the rulers in Kiev, in the sense of guiding Ukraine's course in a certain geopolitical direction.

Particularly relevant is Vladimir Putin's speech during the NATO-Russia Council meeting held on the sidelines of the NATO summit, in which he even brought up the territorial integrity of Ukraine, declaring that" [...] *Ukraine is a very complicated state. Ukraine, in the form it currently exists, was created in Soviet times, it received its territories from Poland – after the Second World War, from Czechoslovakia, from Romania – and at present not all the problems issues have been solved as yet in the border region with Romania in the Black Sea. Then, it received huge territories from Russia in the east and south of the country. It is a complicated state formation. If we introduce into it NATO problems, other problems, it may put the state on the verge of its existence. Complicated internal political problems are taking place there. We should also act very, very carefully. We do not have any right to veto and, probably, we do not pretend to have. But I want that all of us, when deciding such issues, realize that have there our interests as well. Well, seventeen million Russians currently live in Ukraine.*

Who may state that we do not have any interests there? South, the south of Ukraine, completely, there are only Russians" (Text of Putin's speech at NATO Summit, 2008).

What President Putin says is contradicted by Kant through the second article of the peace essay: *"No independent states, large or small, shall come under the dominion of another state by inheritance, exchange, purchase or donation"* (Kant, 2008, p. 64). From the Kantian perspective, a state represents the community of people, to which no one else can dictate except their own conscience. Annexing this state means denying its existence as a collective moral person.

Analyzing Russia's large-scale war of aggression in Ukraine, we can observe a war of conquest initiated by Moscow, a neo-colonial war, of the metropolis against the former component that wants to break away completely – Ukraine, a state that is waging its true war of independence. The course already seems clear to some who are more concerned, of course, not to humiliate Russia than with the victims it is causing in Ukraine and the war crimes or the act of aggression of which it is guilty. Of course, no one sets out to humiliate Russia, but, for its own good and the future of its citizens, it must be defeated and, subsequently, held accountable (Chifu, 2023, p. 19). This is necessary because *"No state shall by force interfere with the constitution or government of another state"* (Kant, p. 66).

After the Orange Revolution in Ukraine, in December 2004, the new leadership in this country expressed its intention of European integration of Ukraine and of continuing efforts to create a state of law based on the principles of a market economy. Ukraine is one of the ENP member states (European Neighbourhood Policy) that signed, in February 2005, an Individual Action Plan with the EU.

The resilience of the Ukrainian society comes from multiple sources and is an element of inspiration from which we can learn. Resilience finds its foundations in society. Society generates reserve forces in large-scale, long-term war. This is a lesson to learn! But what also matters is the motivation to wage a war and to accept the destruction of one's own territory for a higher goal – real independence, the survival of the nation, identity, prestige and national dignity. Resilience is about both the front line, the ability, will and desire to fight, and what happens behind the front line – the population's support for the war effort. The patriotism, bravery, self-denial and self-sacrifice of a nation cannot be replaced by anything else.

In a Kantian perspective, resilience finds its foundation and relevance in the conditioning of a state of peace: this is not a state of beginnings, but one acquired through legal means, mutually guaranteed by neighbouring states. In a situation where civil life is legislated, the law can end hostilities in two ways: either by coercing the neighbour, or by coercing them to leave their neighbourhood, each

preserving their own social existence. The lack of a constitution and civil law, however, makes the one who lives outside them, by their way of living unfettered, inconvenient to the one who has opted for coercion and civil freedom.

In Kantian terms, the resilience of Ukrainian society derives its relevance from the purity of the republican constitution, grounded in the original social contract as articulated within the concept of law. Being founded on the principle of freedom and equality of citizens, in the matter of declaring a war, the citizens of this society are the ones who bear the burden of the struggle: war expenses, the repair of the destruction caused and, last but not least, the debts contracted.

All of these have a common goal: freedom and the ability to live freely within their borders. Freedom can also be translated into the ability to disapprove, to allow the leap towards perfection. It is the instrument of human dignity under the condition of the appropriation of moral law (Kant, p. 46).

Victory and peace in Ukraine depend on this capacity of Western democratic societies to support the war. In fact, if we want to have peace, it does not mean moving towards excessive negotiations and concessions. This is not peace. Peace is not the absence of war at a given moment. It is the situation in which no one challenges the limits created by international law. Peace implies respect for the rules-based international order, the fact that these rules can be imposed, as well as the capacity and political determination to enforce these rules. The war in Ukraine has demonstrated that credible deterrence results from the combination of capabilities and political will – that is, the desire and determination to fight – rather from that sheer strategic weight or numerical superiority.

Unlike Rousseau, for whom the solution to war is a social one – the establishment of a beneficial society meant to correct the principle vice of real society – the corruption of humanity's positive moral core in the natural state; international confederations do not have, within this political theory, the maximum value that the Kantian *Weltanschauung* offers them, where the perspective is the opposite, because war is rooted in human nature and, therefore, the ideal state lacks the means to master it; only an international league could bring about perpetual peace, not through the concerted efforts of human beings, but through the hidden plan of nature, acted upon by two non-moral factors: catastrophes and the convergence of selfish interests.

From a Kantian perspective, there can be no logical international order without an international public law. The Kantian moral imperative conditions peace, because it expresses the moral *summum*, morality being a social and, therefore, political excellence, as the community formed according to moral principles restricts and suppresses phenomena that contradict moral principles. For Kant, the struggle between individual desires and the moral law characterizes man in general and at all times.

HOBBESIAN WAR TENDENCIES AND KANTIAN PERSPECTIVES ON THE UKRAINE – RUSSIA CONFLICT. COMPARATIVE ANALYSIS

Both *Leviathan* and *Perpetual Peace* appeared either in the aftermath of a war or during the course of one, a fact that draws attention to the relevance of these works in the current context of the conflict unfolding on the territory of Ukraine². The difference of more than one hundred years between the moments of their publication is thus diminished, since both bring to the forefront an ontological approach to war from a strictly anthropological perspective. Both authors are concerned with an introspective analysis of the human being and of human behaviour in times of hardship, circumstances that only war can provide.

The invasion of Ukraine by the Russian Federation tends to become the most important military conflict after the Second World War. The Russian-Ukrainian war is not just a regional war. It is the war that marks a rupture in the relations between Russia and the West, a war that will have profound repercussions for both Europe and the entire world. Its global consequences will be considerably greater than the September 11 attacks. For the first time, a military conflict has the potential to involve Russia, NATO and China. Russia and the NATO states have already positioned themselves and are active parties in the conflict, but China seems, for now, undecided.

According to several specialists, Russia seeks to present itself as an authoritarian leader that has stepped out from the forefront of creativity, economic and technological competition and geopolitical capacity through its own destructive manner of managing creative energies and of closing the system in order to preserve the Putinist regime, as well as through the power of a leader who aspires to be more long-lived than Stalin (Chifu, p. 19).

At the beginning of 2022, the situation in Eastern Europe was particularly volatile and complex, being amplified by the spread of the Covid-19 pandemic and the implementation of drastic restrictive measures by the states in the region, in order to escape the fifth wave of infections. In addition, the preconditions for the outbreak of global economic, financial and social crises, not just in this region, had already been outlined. We can also take into account the fact that, throughout 2021, the situation on the border with Ukraine significantly worsened, with the Kremlin intensifying its military presence in the area and conducting joint operational and strategic level exercises with Belarus, including nuclear missiles.

² *Leviathan* was published during the English Civil War (1642-1651), and *Perpetual Peace* following the Franco-Prussian War, concluded by the Peace of Basel on 5 April 1795 (Author's note).

This strategic repositioning of Russian troops near the Ukrainian borders and the increase in its nuclear deterrence posture took place against the backdrop of the operationalisation of the Russian Federation's anti-access/area-denial systems of in the Black Sea, the eastern Mediterranean Sea, the Baltic Sea and the Arctic Ocean, which began after the hybrid war waged by Russia in Ukraine. Thus, during the operational-strategic exercise "Zapad (West) 2021" in western Russia and southern Belarus, the Russian military forces on the border with Ukraine significantly changed, by bringing approximately 20,000–30,000 troops and equipment from other districts and relocating them to training grounds near the western border. In its report of 28 July 2021, the American Center for Strategic and International Studies (CSIS) concluded that: "... *taken together, the scale of the Russian build-up near Ukraine this year [2021] suggested that Russian forces were prepared to undertake deep offensive operations, rather than be used simply as a deterrent against perceived Ukrainian attempts to retake Donbas*" (Ioniță, 2023, p. 11).

As the security relationship between Russia and the West has deteriorated in recent years, Europe and the West have pursued a dual approach. On the one hand, the West has sought to maintain dialogue with Russia and pursue a political solution in Ukraine through the Minsk Process. On the other hand, NATO has taken steps to strengthen its deterrence capability, particularly along its eastern flank. Through the *Enhanced Forward Presence (EFP)* initiative, it has deployed additional, rotational forces to Poland and the Baltic states. Europe has also maintained relative unity on a number of issues in its relations with Russia.

For more than seven years, EU sanctions against Russia for its actions in Ukraine have remained in place, and additional EU sanctions followed the poisoning of opposition leader Alexei Navalny with Novichok in 2020. This situation has, in our view, seriously affected the level of trust in Russia, which can be analyzed through a Kantian perspective in the following way: "*No state shall, during war, permit such acts of hostility which would make mutual confidence in the subsequent peace impossible: such are the employment of assassins (percussores), poisoners (venefici), breach of capitulation, and incitement to treason (perduellio) in the opposing state*" (Kant, p. 67).

These are dishonourable stratagems. Even during a war, it is essential to maintain a level of trust in the enemy's way of thinking, otherwise no peace could be concluded, and hostilities would degenerate into a war of extermination (*bellum internecinum*); in the natural state, war is only a sad emergency means by which a state defends its right to freedom and the free decision of its own destiny.

The image of Russia finds its counterpart in Hobbesian language through the iconic representation of the Leviathan, the well-known biblical monster that we learn about in the Book of Job as being without equal. Hobbes also presents it in this manner, with some of the following attributes: instability, intolerance and lack of peace/freedom. Changing the paradigm while retaining Hobbesian concepts, this analysis can also be applied to the image that Russia, whose expansionist tendencies have been manifesting in the most repulsive way. Through its actions, Russia has generated a complex and profound state of instability, undermining the peace and freedom of Ukrainian society, with consequences for an indeterminate period for the future.

Russia's instability and unpredictability represent a different status from that of other countries in Eastern Europe, because it implies that these will soon be implicit problems of the European Union; they could block the EU's expansion and provoke a crisis within it: also, the states of Eastern Europe are perceived as being similar to Western ones.

CONCLUSIONS

The transformations that have taken place in the international security environment over the past decade, especially in its most recent period, have focused the attention of the international community on clarifying a vision that would contribute to the consolidation of world peace and security, therefore to the reduction of conflict situations of any nature, implicitly, to the reduction, until elimination, where possible, of the causes that generate them.

The influence of Hobbes, in general, and of *Leviathan*, in particular, on subsequent eras is difficult to assess, mainly because many authors have failed to acknowledge the extent of their influence coming from the English philosopher, often fearing accusations of atheism or "*Hobbism*". Despite some ideas that remain a testament to the era in which he lived and the logic he adopted (such as the theory of absolute power or the public censorship of subversive writings) and regardless of whether or not he is considered an unwitting precursor of liberalism, many of Hobbes' ideas have demonstrated their primacy and even modernity.

War, regardless of its nature, as well as concepts such as political stability, individual freedom, freedom of conscience, education and peace are just a few of the concepts that preoccupied Thomas Hobbes, thus providing us with the necessary framework through which to analyse the war launched by the Russian Federation in Ukraine. Of course, it is not the only or perhaps the most appropriate way to examine this important conflict, but what is striking is that more than three

centuries after Hobbes managed to make his work known, human society, in terms of certain customs, appears to have changed little, a context in which the perspective announced in the title also intervenes: that of anthropology. Through this article, we aim to bring to attention facts that have been recognised for more than three centuries and, with or without science, have been manifested by the protagonists of the Russian-Ukrainian war.

By bringing these aspects to attention, we seek to raise the question of how long it takes for humanity to prove the progress it has achieved, if in the face of contexts, such as that of the conflict presented here very succinctly, we continue to witness the relevance of works written long ago, and in this sense, *Leviathan* serves or may serve as simple example. Certainly, a more thorough research might reveal older studies or works better suited to contextualising the Russian-Ukrainian conflict from an anthropological perspective.

Perpetual Peace, due to the hopes that its humanist message of universal peace and equity instils, is – among Kant’s short works – one of the most cited and read. Between dream and reality, “*perpetual peace*” leads us to think of the hope of the ordinary person to someday reach – through the absence of social conflicts – the state of maximum prosperity. From Kant’s point of view, the state of peace is not a state of beginnings, but one acquired through legal means, mutually guaranteed by neighbouring states. Reason condemns war in the name of moral law, making the establishment of peace an immediate duty, based on a contract between peoples.

From our perspective, Ukraine, and the manner in which Ukrainian society faces this war, unwanted even in the darkest of dreams, fits the pattern presented by Immanuel Kant through the point of view of the desire for respect of sovereignty, territorial integrity, individual freedom, freedom of thought and, last but not least, the capacity for self-determination.

Regarding this context, we adhere to Kant’s view that when a large and powerful state has expansionist tendencies towards another, smaller state, the latter is justified in defending itself even through attacks launched against the invader, without having first committed any offense. Also, from a Kantian perspective, the attacked state has every right to seek any alliances necessary to escape the terror imposed by the invader, in order to restore, although with great difficulty in the case of Ukraine, the initial state of affairs.

BIBLIOGRAPHY:

1. Barret, A.A. (1993). *Calligula. The Corruption of Power*. New York: Editura Routledge.
2. Cebotari, S. (2022). *Impactul războiului ruso-ucrainean asupra relațiilor internaționale*, in *Moldoscopie*, nr. 1, pp. 65-78.

3. Chifu, I. (2023). *Securitatea, apărarea și pacea pe flancul estic. Lecții învățate din conflictul din Ucraina*, in *Infosfera*, nr. 2, p. 19.
4. Churchill, W.S. (1973). *The Sinews of Peace: Post-War Speeches*, ed. by Randolph S. Churchill, Houghton Mifflin Co., London.
5. dictionar-citate.blogspot.com (2011), retrieved on 22 August 2025.
6. Diez, Th., Stetter, S., Albert, M. (April 2004). *The European Union and Border Conflicts: The Transformative Power of Integration*, presentation delivered during the European Consortium for Political Research Joint Sessions in Uppsala, Sweden.
7. Hobbes, Th. (2023). *Leviatanul*, translation, foreword and notes by Alexandru Anghel. București: Editura Herald.
8. Ioniță, C.C. (2023). *Convențional și hibrid în primul an al războiului Federației Ruse împotriva Ucrainei. Concluzii și lecții desprinse din război*. București: Editura Universității de Apărare “Carol I”.
9. Kant, Im. (2008). *Spre pacea eternă. Un proiect filosofic*, translation and introductory study by Rodica Croitoru. București: Editura All.
10. Maciej, M., Paszkowsky, M. (2023). *Russia's Falin – Kvitsnisky Energy Doctrine. History and Experience Applying to Selected Central European Countries*, in *Torun International Studies*, vol. I, nr. 18, pp. 69-82.
11. Matei, Gh. (2022). *Federația Rusă: vectori ai politicii externe pe direcțiile strategice vest și sud-vest*, in *Infosfera*, year XIV, nr. 3, pp. 29-36.
12. Roșu, C., *Rusia pierde în Ucraina puterea de negociere cu China și apartenența la spațiul european*, https://adevarul.ro/international/europa/rusia-pierde-ucraina-putereade-negociere-china-apartenenta-spatiul-european-1_6258fbf75163ec4271633dbe/index.html?fbclid=IwAR0xpms8hfRiargVzJo9crPXfAV3WApX19OqBUQfMq8gOCUZunM9bfVichU, retrieved on 5 mai 2022, apud Cebotari, S. (2022). *Impactul războiului ruso-ucrainean asupra relațiilor internaționale*, in *Moldoscopie*, nr.1, pp. 65-78.
13. Sakwa, R. (2008). *Russian Politics and Society*, 6th edition, London: Routledge.
14. Sarcinschi, A., Dinu, M. (f.a.). *Crize și instabilitate în Europa*. București: Universitatea Națională de Apărare, Centrul de Studii Strategice de Apărare și Securitate.
15. Shotter, D. (1992). *Tiberius Caesar*. New York: Editura Routledge.
16. Ștefan, Al. (2021). *Mutații în sistemul internațional în contextul conflictului în Siria. Posibile scenarii de resetare a balanței de putere*, doctoral thesis. București: Școala Națională de Studii Politice și Administrative, Școala Doctorală de Științe Politice.
17. Text of Putin's speech at NATO Summit (Bucharest, 2 April 2008), UNIAN, retrieved on 14 August 2025.
18. Tinguy, A. de, coord. (2008). *Moscova și lumea. Ambiția grandorii: o iluzie?* București: Editura Minerva.
19. Ziegler, Ch.E. (2020-2021). *A Crisis of Diverging Perspectives: U.S.-Russian Relations and the Security Dilemma*, Texas National Security Review, retrieved on 13 August 2025.
20. <https://russiancouncil.ru/en/analytics-and-comments/analytics/how-to-stop-nato/>, retrieved on 10 August 2025.
21. <https://www.brookings.edu/articles/10-maps-that-explain-ukraines-struggle-for-independence/>, retrieved on 12 August 2025.

SHIPS SUNK IN THE BLACK SEA DURING THE RUSSIAN-UKRAINIAN WAR (2022-2025) – LESSONS FOR NAVAL STRATEGY AND TACTICS –

Navy Captain (Ret.) Associate Professor Dr. Romeo BOȘNEAGU

Naval Academy "Mircea cel Bătrân", Constanța

DOI: 10.55535/RMT.2025.3.08

Between February 2022 and mid-2025, the Black Sea became a testing ground for the naval warfare of the present and the future. This new reality, unimaginable in the recent past, forced the relocation of ships and naval military equipment, limited maritime control, while maritime freight transport faced new, high-impact risks because of naval mines and attacks by belligerents.

Cataloguing confirmed sinkings of military and commercial vessels (names, classes, locations, and dates) has allowed lessons to be learned about modern naval warfare, ships versus drones and ships versus missiles, in a semi-enclosed sea governed by the Montreux Convention.

Keywords: Russian Federation's naval forces; Black Sea; Ukrainian Navy; mine protection measures; Turkey-Romania-Bulgaria MCM Working Group;

INTRODUCTION

The Black Sea, a natural inland basin on the border between Europe and Asia, is important for Europe due to: its geographical position, which is now recognized as being of geostrategic importance; its surface area of over 420,000 km²; its volume of over 547,000 km³; its maximum depth of 2,212 m; a coastline of over 4,800 km; a coastal population of over 160 million, with 18 major ports and 10 major rivers in its hydrographical basin; a total freshwater flow of over 350 km³/year and rich energy sources (current, wind, hydrogen sulphide).

The Black Sea has the appearance of a deep basin, oriented from west to east, stretching approximately six degrees of latitude between the parallels: 40°55'N and 46°37'N, and five degrees of longitude between the meridians: 27°27'E and 41°47'E (figure 1).

The Black Sea is considered an intercontinental sea, with access to the Mediterranean Sea through the Bosphorus Strait and to the Sea of Azov through the Kerch Strait. Due to its geography, it is thus positioned to represent a water link between East and West, a link between Europe and Asia, between coastal states and those in the immediate and distant proximity (Bosneagu, 2022).



Figure 1: The Black Sea – geographical position (ro.wikipedia.org/wiki/Marea_Neagra)

Between February 2022 and mid-2025, the Black Sea became a testing ground for anti-ship missiles and unmanned surface vessels (USVs). Ukraine's coastal missile complex, together with MAGURA-V5 USVs, caused substantial losses to the Russian fleet in the Black Sea, forcing the relocation of Russian ships from Sevastopol and limiting maritime control. The Black Sea straits (Bosporus and Dardanelles) and Turkey's invocation of Article 19 of the Montreux Convention in 2022 restricted the transit of belligerent warships, limiting reinforcements and amplifying the effect of each loss (Reuters, 2023). In this context, Ukraine used long-range missiles and USVs to strike BSF warships at sea and in port, contributing to the relocation of the fleet to the east and a reduction in combat strength by about one-third by 2024-2025, according to widely cited sources (Royal United Services Institute, 2025).

MATERIALS AND METHODS

The main sources of information and analysis include: a. international media institutions: a. Reuters/AP, (<https://www.reuters.com/company/associated-press/>), USNI News (<https://www.usni.org/magazines/proceedings>), Naval News (<https://www.navalnews.com/category/naval-news/>), RUSI assessments (<https://www.rusi.org/news-and-comment>), b. official sources of the combatants: TASS (<https://tass.com/>), The Moscow Times (<https://www.themoscowtimes.com/>), Ukrainform (<https://www.ukrinform.net/>), Kyiv Post (<https://www.kyivpost.com/>), Ministry of Defence of Ukraine (<https://mod.gov.ua/en/news>, <https://mod.gov.ua/en/about-us/the-general-staff-of-the-armed-forces-of-ukraine>), c. international encyclopaedic sources for data verification: Britannica (<https://www.britannica.com/>).

The classic rule of research data confirmation was applied: a ship appears on the list of sunken ships only when its sinking/destruction (not just “*damage*”) is confirmed by several reliable sources.

RESULTS AND DISCUSSIONS

An analysis of the strength of the Russian Federation's naval forces in the Black Sea versus that of Ukraine's naval forces prior to 2022 shows the clear superiority of the Russian forces (*table 1* and *figure 2*).

Ships Sunk in the Black Sea During the Russian-Ukrainian War (2022-2025)
– Lessons for Naval Strategy and Tactics –

Table 1: Russian Navy versus Ukrainian Navy before 2022 (Jane's Fighting Ships, 1999)

Ship	Russian Federation	Ukraine
Missile cruiser	1 Slava Class, displacement 11,674 t	
Missile destroyer	1 Kashin Class, displacement 4,826 t	
Frigate	3 FFG Krivak Class, displacement 3,709 t	1 FFGHM Class, displacement 2,500 t
SSK submarine, patrol submarine with ASW capability	3: 1 Kilo Class, 2 Varshavyanka Class	1 Foxtrot Class, displacement 2,475 t
Corvettes	15	
Anti-submarine corvettes	5	
Missile boats	6	4
Minesweepers Mine hunters	10	
Minelayers		1
Torpedo boats		
Landing craft vessels	7	
Patrol vessels		2
Reconnaissance ships		2
Training vessels		
Auxiliary vessels	13	21
Aircraft	20 helicopters, 10 transport aircraft 2 fighter squadrons	
Naval bases	Sevastopol, Tuapse, Novorossiysk, Feodosia	Odessa, Novozerne, Mikolaiv, Feodosiya, Izmail
Personnel	11,000 (including marines)	14,800

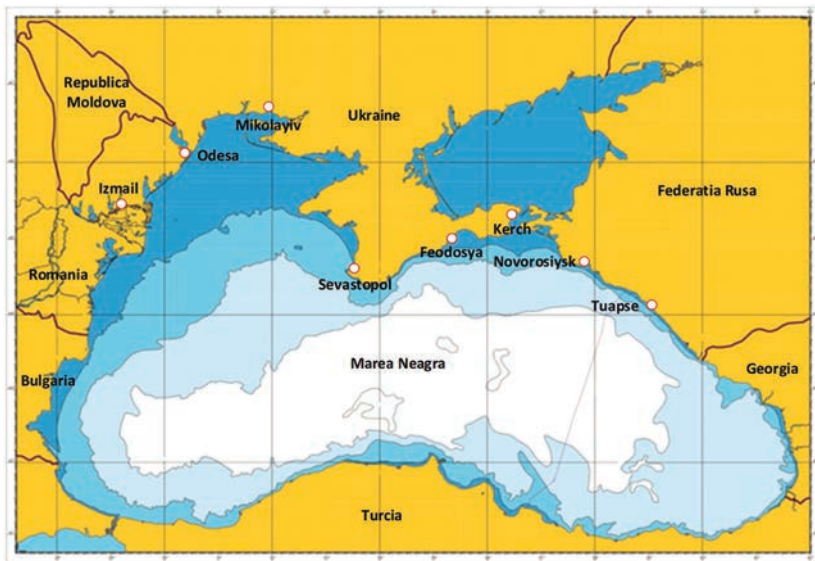


Figure 2: Russian Federation, Ukraine – naval bases in the Black Sea
(ro.wikipedia.org/wiki/Marea_Neagra)

At the beginning of the war, the Russian Federation Navy, although numerically and technically superior to the Ukrainian Navy, was moved from Crimea (Sevastopol) by 2024, with approximately 25-33% of its combat capacity destroyed or neutralised, according to international estimates (Royal United Services Institute, 2025).

With limited traditional naval resources, Ukraine resorted to unconventional means of combat (modernised anti-ship missiles, surface and submarines drones) to block the asymmetric access of Russian naval forces at sea (Reuters, 2025).

Due to its inferiority in terms of conventional naval warfare capabilities (medium and large ships equipped with missiles and heavy naval weapons), Ukraine has employed a novel approach to maritime warfare using unconventional means that are technically and tactically superior to Russian ones, fast, inexpensive, and relatively simple to use in combat, remotely controlled, difficult to detect and counter, relatively simple to use in combat without human loss (*table 2*).

Table 2: Unconventional means used by Ukraine in naval warfare in the Black Sea, 2022–2025

Means of combat	Technical and tactical characteristics
Magura V5	5.5 m long, 1.5 m wide, 0.5 m above the waterline, 22 (minimum) 42 (maximum) knots speed, 450 nautical miles range, 320 kg payload, radio and satellite communications

Ships Sunk in the Black Sea During the Russian-Ukrainian War (2022-2025)
– Lessons for Naval Strategy and Tactics –

Means of combat	Technical and tactical characteristics
Bayraktar TB 2	Medium-altitude, long-endurance (MALE) unmanned tactical aerial vehicle capable of performing intelligence, surveillance and reconnaissance (ISR) missions and armed attack missions, operational altitude 16,000 feet, payload capacity 150 kg, wingspan 12 m, length 6.5 m, height 2.2 m
Sea Baby	length: 6 m, width: 2 m, height above waterline: 0.6 m, maximum speed: 49 knots, range: 540 nautical miles with additional fuel tanks, payload: 850 kg, propulsion: two 200 hp internal engines, satellite communications, can carry RPV-16 thermobaric missiles, unguided, with a range of approximately 1,000 m
R-360 Neptune, anti-ship missile	development of the Soviet Zvezda Kh-35 (SS-N-25 SWITCHBLADE) anti-ship missile, weighing 870 kg, length 5.05 m, maximum range of 400 km (combat weight of 150 kg for the anti-ship version), guided by satellite and, in the final part of the flight, by an infrared guidance system

Analysis of naval actions in the Black Sea between 2022 and 2025 led to ship losses for both belligerent forces, after verification of the information, as follows (*tables 3 and 4, figure 3*).

Table 3: Losses of military ships in the naval war in the Black Sea, 2022-2025

Ship	Date and position	Russian version	Ukrainian version	Details
Russian ships				
<i>Moskva</i> , missile cruiser	13/14 April 2022; approx. 80 miles south-west of Odessa	A fire caused an ammunition explosion, and the ship sank in stormy seas while being towed to port	Hit by 2 <i>R-360 Neptune</i> anti-ship missiles	Of the 485 crew members, casualties vary depending on the source (Russian sources initially reported 1 and then 27 missing, while other sources claim that only 58 sailors were rescued). According to unverified open sources, there were two 350-kiloton nuclear warheads on board the ship – information that has been unconfirmed or denied

Ship	Date and position	Russian version	Ukrainian version	Details
Five Raptor-class patrol boats	22 March 2022		hit and damaged by an anti-tank guided missile	
Two Raptor-class patrol boats	2 May 2022; near Serpent Island		sunk by a Bayraktar TB2 drone	
<i>Saratov</i> , Russian Navy Alligator-class landing ship	24 March 2022; in Berdiansk	was sunk in March by its own crew, then recovered and was to be towed to Kerch	it was hit, caught fire and destroyed	
BK-16 High Speed Assault Boat	May 2022; near Serpent Island		sunk by a Ukrainian Bayraktar TB2 drone	
Serna-class landing craft	7 May 2022; near Serpent Island		sunk by a Ukrainian Bayraktar TB2 drone	
<i>Vasily Bekh</i> rescue tug	17 June 2022		sunk by 2 Harpoon missiles	
<i>D106 Ondatra</i> -class landing craft	July 2022		sunk by a sea mine	
<i>Ivan Golubets</i> Natya-class minesweeper	29 October 2022	slightly damaged by Ukrainian UAVs	sunk by a Ukrainian UAV	
<i>Admiral Makarov</i> frigate	29 October 2022	15 August 2023, entered service	hit by Ukrainian drones	
<i>Ivan Khurs</i> intelligence ship	24 May 2023		possibly hit by 1 to 3 drones	23 March 2024, hit by a missile in Sevastopol
<i>Olenegorsky Gornyak</i> landing ship	4 August 2023		heavily damaged by a marine drone	
<i>Rostov-on-Don</i> landing ship	13 September 2023; Sevastopol	repaired, operational	hit by air-to-surface missiles	

Ships Sunk in the Black Sea During the Russian-Ukrainian War (2022-2025)
– Lessons for Naval Strategy and Tactics –

Ship	Date and position	Russian version	Ukrainian version	Details
Minsk submarine	13 September 2023; Sevastopol	repaired, operational	hit by air missiles	
Tuna-class patrol boat	13 September 2023; in the north-western part of the Black Sea		sunk by a Ukrainian Bayraktar TB2 drone	3 September 2023 Ukrainian forces claimed to have sunk another Tuna-class patrol boat with Ukrainian Bayraktar TB2 drones
<i>Sergey Kotov</i> patrol ship	14 September 2023		damaged in an air strike	5 March 2024, it was sunk by a Ukrainian unmanned surface vehicle near the Kerch Strait
<i>Askold</i> corvette	4 November 2023; Zalyv		destroyed in an air strike	
<i>Novocherkassk</i> landing ship	26 December 2023; Feodosia harbour		destroyed in an air raid	massive and multiple explosions and fires; 74 crew members reported dead and 27 wounded; wreckage apparently removed in late January/early February 2024
<i>Ivanovets</i> corvette	1 February 2024; Donuzlav, in the western part of the Crimean Peninsula		sunk by an AUV	
<i>Tsezar Kunikov</i> large landing ship	14 February 2024; on the coast of the Crimean Peninsula	confirmed sinking	sunk by an AUV	

Ship	Date and position	Russian version	Ukrainian version	Details
Mangust-class patrol boat	6 May 2024		a drone exploded near a small boat that appears to resemble a Mangust-class vessel	
<i>Saturn</i> tugboat	6 June 2024		sunk by a Ukrainian sea drone	
Ukrainian ships				
A206 <i>Vinnytsia</i> auxiliary ship	24 February 2022	sunk at anchor		
Eight unidentified vessels	26 February 2022	reported as destroyed		
<i>F130 Hetman Sahaidachny</i> frigate	3 March 2022		sunk in Mykolaiv to prevent its capture by the Russian Navy	
<i>P190 Sloviansk</i> patrol boat	3 March 2022	sunk by an air-to-surface missile		
<i>Henichesk (M360)</i> minesweeper	August 2022		lost in the early stages of the Russian invasion	
about a dozen Ukrainian ships captured by Russian Navy	14 March 2022; Berdiansk and Mariupol			captured: artillery ships, missile ships, a corvette, a patrol ship, a minesweeper, a landing ship, a sea tug
<i>A512 Pereyaslav</i> reconnaissance ship	30 March 2022; Dniester	destroyed by artillery fire		
Dmitry Chubar hydrographic boat	20 May 2022	captured in the port of Mariupol		
<i>L450 Stanislav</i> fast assault craft	29 November 2022		losses during the Ukrainian counteroffensive on 7 May on Serpent Island	

Ships Sunk in the Black Sea During the Russian-Ukrainian War (2022-2025)
– Lessons for Naval Strategy and Tactics –

Ship	Date and position	Russian version	Ukrainian version	Details
16 to 24 attack/reconnaissance USVs	September 2022	captured and subsequently destroyed		
Several USVs	November 2020 - June 2023	destroyed during Ukrainian attacks		
PO-2 small patrol gunboat	17 April 2023	destroyed		
Centaur LK assault craft	26 June 2023	damaged in port		
Ship	28 August 2025; in the Danube Delta	sunk by a marine drone		

Table 4: Losses of military ships in the Black Sea war, type and number, 2022-2025

Type	Russia	Ukraine
Cruiser	1	-
Frigate	-	1
Corvette	-	2
Patrol vessel	3	6
Artillery-carrying boat	-	6
Assault ships	1	1
Command ship	-	1
Landing craft, medium	1	1
Small landing craft	1	-
Mine layer	-	1
Tugboat	2	-
Hydrographic vessel	-	1
Number	9	20
Tonnage	Approx. 10,000 t	Approx. 10,000 t



Figure 3: Russian Cruiser Moskva, before and after being hit by Ukrainian missiles
(<http://www.navylookout.com/russian-cruiser-moskva-sunk-in-the-black-sea-assessing-the-implication/>?)

During the naval war in the Black Sea, 2022-2025, a significant number of commercial ships were sunk (*table 5*).

Table 5: Commercial ships lost during the war in the Black Sea, 2022-2025

Ship	Type of ship, location and date
Yasa Jupiter	Bulk carrier hit by a Russian forces' missile, off the coast of Odessa, Ukraine, on 24 February 2022, damaged
Millennial Spirit	Chemical tanker bombed off the coast of Ukraine, on 25 February 2022, caught fire and sank
Helt	Cargo ship sunk off the coast of Ukraine on 2 March 2022, probably after hitting a mine or being sunk by a Russian missile
Azburg	Cargo ship bombed and sunk on 4 April 2022 during the battle of Mariupol, after being damaged the day before by two Russian missiles
Vyssos	Cargo ship hit a naval mine on 27 December 2023 off Bystre, at the entrance to the Danube Delta; the ship was beached to prevent it from sinking
Simferopol	Ship sunk after a naval drone attack in the Danube Delta on 28 August 2025

In addition to these commercial ships, there were many others that were hit by enemy fire, damaged in various ways, and suffered human losses on board.

The war is not over, Ukraine has continued research and testing for new means of combat (new types, with increasingly advanced technical and tactical characteristics/*table 6*). They are currently undergoing approval and will probably be used in future naval operations. They can be a source of inspiration for analysing the need to develop new naval weapons.

Some of these new weapon models are capable of travelling over 1,500 km and can carry up to 2,000 kg of explosives. They can also carry a multiple rocket launch system.

Ships Sunk in the Black Sea During the Russian-Ukrainian War (2022-2025)
– Lessons for Naval Strategy and Tactics –

Table 6: New naval weapons developed by the Ukrainian Navy

Type	Characteristics
Magura W6	USV equipped with an improvised air defence system using the Sea Dragon system, whaler hull, consisting of two AA-11 ARCHER (R-73) missiles
Magura V6	USV similar to V7 and can carry the Sea Dragon air defence system with Sidewinder or AA-11 ARCHER missiles
Magura V7	Slightly larger, with a length of 7.5 m, can carry two AIM-9L Sidewinder air-to-air missiles. Similar to the V5, but redesigned with improved stability at sea, useful for winter operations, with multiple communications antennas and sensors
Toloka TLK-150	USV equipped with explosives, designed to function as a torpedo, with a typical tubular body, but with a large keel and horizontal stabilizers, with thrusters at the end of these stabilizers for propulsion and manoeuvring. With a mast above the water, it can be defined as a semi-submersible. There may be several versions, including one with a length of 4 m, a predictable range from 400 km to 1,200 km
Toloka TLK-1000	Much larger than the TLK-150, 12 metres long, 2,000 km range, and a maximum payload of 5,000 kg
Sea Baby-2, 'Avdiivka'	An explosive payload of 400 kg., 500 nautical miles range and a 48 knots speed. A reinforced hull for 1.5 metres high waves draught approximately 1 metre, and a height of 1 m above water. Communications by satellites
Sea Wolf	Larger than the Sea Baby, is offered with a wide range of weapon configurations
Stalker 5.0	Characteristics: 5 m long, 1.2 m wide, a payload of 150 kg. 60 Hp outboard motor, 40 knots maximum speed, 350-600 km range
Marichka Underwater Drone (AUV)	Large autonomous underwater vehicle (AUV), probably the first created directly from the needs of war. The base vehicle is 6 metres long and 1 metre in diameter, 1,000 km range, with all or most of the body being a pressure vessel. A keel appears to run along the bottom, and tow loops are located at the rear. For combating ships, bridges, gathering information and transport
Weaponized AM-800 RHIB	An unidentified USV was discovered, overturned, in Romanian waters on 3 April 2024. The vessel is based on an American-made Silver Ships AM-800 rigid-hulled inflatable boat (RHIB). The warhead came from a STYX anti-ship missile.

Type	Characteristics
Riverine Resupply USV	The logistics USV prototype was observed with two ammunition containers (American type, 120 mm or 155 mm cartridges). The vessel is very small, with a length of approximately 1.5 metres and a payload of 30 kg.
Katran X1	length: 8 metres, width: 2.3 metres, height above the waterline: 1.2 metres, speed: 56 knots max, 32 knots cruising, range: 650 nautical miles at cruising speed, payload: 4 10" FPV drones, "Osa" attack drones, propulsion: 1 outboard motor, satellite communications
Katran X3	length: 6.5 metres, width: 2.2 metres, height above waterline: 1.1 metres, speed: 40 knots max, 30 knots cruising, range: 890 nautical miles (1,650 km) at cruising speed, payload: 4 FPV drones, internal strike payload, propulsion: 1 outboard motor, satellite communications
Alligator	small naval drone, approximately the size of a jet ski, with a faceted shape
Barracuda	for river and coastal operations in support of sailors, equipped with 4 or more shoulder-launched RPG-26 missiles
Unnamed type with missile tubes	has two launch tubes, one on each side of the body. These look similar to torpedo tubes, but are more likely intended for missiles. Possibly a Katran Venom

Table 7: Russian drones (2022–2025) – characteristics and operational status

Name	Type/role	Technical characteristics	Operational status	Comments
Murena-300/300S	Medium USV, multi-role	5.5 m long; speed 40-45 kn; range ~500 km; payload up to 500 kg	Confirmed use (Pivdenne attack, 2024)	The only USV with documented actual combat use
Orkan	Lightweight, multi-role USV	~5.3 m; speed 40 kn; range 500 km; modular payload	Unconfirmed in combat	Presented at the exhibition, appears to be oriented towards reconnaissance/anti-USV
Vizir (RK-700)	Heavy, multi-role USV	~7 m; range 500–800 km; can integrate missiles	Demonstration only	Robust platform but not validated in real conditions

Name	Type/role	Technical characteristics	Operational status	Comments
BEK-1000	Logistics/attack USV	Capacity 1000 kg	Prototype/exhibitions	Pilot project for heavy loads

LESSONS IN NAVAL STRATEGY AND TACTICS

Ships versus Missiles

Analysis of the confrontation between missiles and ships shows the following:

❖ The density of salvos and the diversity of modern anti-ship missile guidance and strike systems (modernised Neptune missiles) have overwhelmed the classic anti-aircraft defence systems on Russian ships (e.g. the cruiser Moskva). The requirements for combating this new type of air-naval threat should now include: flexible, computerised, complex, very fast-reacting anti-aircraft weapon systems capable of combating fast, small targets that attack multidirectionally and in waves; reflective means of “blinding” drones, devices for physical camouflage and for reducing the thermal and radio-technical footprint of ships, plus integration with land-based and air defence systems (Reuters, 2025).

❖ The vulnerability of port and naval infrastructure to air and drone attacks and the destruction of ships in port show that berthing and repair areas require reinforced shelters, means of camouflage, deception of the enemy and rapid deployment. The following are also crucial for successful defence: the ability to rapidly disperse forces; means of increasing the mobility of personnel, ammunition and fuel (Ib.).

Ships versus Drones

An analysis of the confrontation between missiles and ships versus drones shows the following:

❖ In terms of detection, classification and success in naval combat, it can be seen how marine drone attacks exploited the weather, time and space: windows of opportunity during the day and night, sea conditions, low-altitude flight, and attacks from multiple directions. Effective countering of marine drones requires layered defence (with guided speedboats, physical barriers around anchored ships, anti-speedboat weapons with a longer range, and areas blocking satellite positioning information). The loss of Russian ships shows the failure of tactics regarding the thinking and organisation of close surveillance and defence (Naval News, 2025).

❖ The cost-benefit analysis favours the attacker: marine drones worth approximately \$0.25-0.5 million endanger ships worth hundreds of millions of dollars; the tactics for implementing effective defence must focus on escort forces, night-fighting sensors, illumination from naval helicopters, and carefully planned denial and defence fire.

Maritime Denial and Trade at Sea

Despite sustained attacks, Ukraine requested and obtained the opening and reopening of corridors for grain exports and restored export volumes to pre-war levels in 2023-2024, showing how a maritime blockade and factors facilitating the continuation of maritime trade during a state of war can coexist (Reuters, 2024).

Sea Mine Warfare and Mine Protection Measures

Floating sea mines have increased the risk of accidents and ship sinkings throughout the entire Black Sea theatre of operations. The Turkey-Romania-Bulgaria MCM Working Group (2024) demonstrates the usefulness of coalitions of coastal states with common rules of action, the exchange of common information on incidents and frequent exercises – an essential model for the post-war normalisation of the naval situation in the Black Sea (Reuters, 2024).

Operational and Tactical Consequences

The Russian Black Sea Fleet has sometimes shown moments of operational inactivity, with reduced reaction, repositioning and freedom of action, proving that land-based missile and drone attacks can neutralise larger fleets in semi-enclosed seas for a time. This is a lesson to be learned for the future here and in other similar theatres of operations.

Implications for the Environment and Navigation Safety

Damaged or sunken warships, as well as attacks on port infrastructure, pose a risk of marine pollution from fuel spills and ammunition losses; Furthermore, drifting sea mines continue to wash ashore or are neutralised at sea, requiring long-term assessment of wrecks and monitoring of the coastline alongside mine countermeasures forces (Ib.).

CONCLUSIONS

The study on Russian and Ukrainian warship losses during the Black Sea war, 2022-2025, is not exhaustive; the data presented and analysed in this article are based solely on information from public sources.

No exhaustive research has yet been conducted on the human and material losses suffered by commercial vessels during the Russian-Ukrainian naval war in the Black Sea, 2022-2025.

The catalogued shipwrecks confirm Ukraine's sustained ability to strike the Russian Black Sea Fleet using missiles and marine drones, while the losses of commercial vessels, although fewer, had a disproportionate impact on insurance and trade.

Ukraine's new naval strategy of compensating for its lack of conventional forces and means with unconventional means has paid off. Surface and underwater marine drones, layered air defence, long-range anti-ship coastal missiles and sea mines provide a powerful deterrent to enemy action and are now basic requirements for coastal defence.

Given their superior technical and tactical characteristics: long range, high precision, high speed, difficult to detect and combat, large combat load in relation to their size, new approaches to naval tactics for the use of these dual-purpose means, both for defence and attack, have been tested.

Trilateral cooperation on mine defence in the Black Sea and transparent management of maritime transport corridors remain essential for the recovery of maritime trade.

BIBLIOGRAPHICAL REFERENCES:

1. Boşneagu, R. (2022). *The Black Sea from Paleogeography to Modern Navigation. Applied Maritime Geography and Oceanography*, Springer, <https://baykartech.com/en/uav/bayraktar-tb2/>, retrieved on 22 August 2025.
2. Braun, K., "Black Sea grain exports beating early market ideas by substantial", Reuters, 2004, <https://www.reuters.com/markets/commodities/black-sea-grain-exports-beating-early-market-ideas-by-substantial-degree-braun-2024-03-11/>, retrieved on 12 August 2025.
3. Lister, T., Butenko, V., Gak, K. (2025). *Jet-powered bombs and planes-turned-missiles: Ukrainian and Russian militaries improvise and adapt in a battle of wits*, <https://edition.cnn.com/2025/10/25/europe/ukraine-russia-militaries-improvise-missiles-intl.>, retrieved on 22 August 2025.
4. Naval News, *Analysis: An Operational View on the USV Attacks in the Black Sea from an Admiral's Eyes*, <https://www.navalnews.com/naval-news/2024/02/analysis->

- an-operational-view-on-the-usv-attacks-in-the-black-sea-from-an-admirals-eyes/, retrieved on 22 August 2025.
5. Naval News (14 February 2024). *Ukraine hits Ropucha-class LST Caesar Kunikov with USV attack*, <https://www.navalnews.com/naval-news/2024/02/ukraine-hits-russias-ropucha-i-class-lst-caesar-kunikov-with-usv-attack/>, retrieved on 22 August 2025.
 6. Reuters (15 April 2022). *How big a loss to Russia is the sinking of the Moskva missile cruiser?*, <https://www.reuters.com/world/europe/how-big-loss-russia-is-sinking-moskva-missile-cruiser-2022-04-15/>, retrieved on 22 August 2025.
 7. Reuters (5 March 2024). *Ukraine says it has sunk a Russian patrol ship near Crimea*, [reuters.com/world/europe/ukrainian-sea-drones-damage-russian-black-sea-fleet-patrol-ship-near-crimea-2024-03-05/](https://www.reuters.com/world/europe/ukrainian-sea-drones-damage-russian-black-sea-fleet-patrol-ship-near-crimea-2024-03-05/), retrieved on 22 August 2025.
 8. Reuters (14-15 April 2025). *Russia says flagship Black Sea warship badly damaged... then sank*, <https://www.reuters.com/world/europe/russia-says-flagship-black-sea-fleet-badly-damaged-by-blast-2022-04-14/>, retrieved on 22 August 2025.
 9. RUSI (14 April 2025). *Black Sea: Significance to European Security*, <https://www.rusi.org/explore-our-research/publications/commentary/black-sea-significance-european-security>, retrieved on 12 August 2025.
 10. Sutton, H.I. (2025), <http://www.hisutton.com/Timeline-2022-Ukraine-Invasion-At-Sea.html>, <http://www.hisutton.com/Ukrainian-USVs-Russo-Ukraine-War.html>, retrieved on 17 July 2025.
 11. The Guardian (5 March 2024). *Ukraine sinks Russian warship in occupied Crimea*, <https://www.theguardian.com/world/2024/mar/05/ukraine-russian-warship-occupied-crimea-sinking>, retrieved on 2 August 2025..
 12. Thorne, S.J., *Black Sea Fleet functionally inactive* (March-August 2024). *Russia's Black Sea fleet falls back amid staggering losses*, Legion Magazine, <https://legionmagazine.com/russias-black-sea-fleet-falls-back-amid-staggering-losses/>, retrieved on 12 August 2025.
 13. Trompiz, G., Polityuc, P., *"Ukraine's Black Sea grain export success tested by Red Sea crisis"*, Reuters (2024), <https://www.reuters.com/markets/commodities/ukraines-black-sea-grain-export-success-tested-by-red-sea-crisis-2024-01-24/>, retrieved on 22 August 2025.
 14. USNI News (25 March 2022). *Satellite Images Confirm Russian Navy Landing Ship Was Sunk at Berdyansk*, <https://news.usni.org/tag/berdyansk>, retrieved on 22 August 2025.
 15. Wertheim, E., *"Ukraine's Magura Naval Drones: Black Sea Equalizers"*, Reuters, 2025, <https://www.usni.org/magazines/proceedings/2025/september/ukraines-magura-naval-drones-black-sea-equalizers>, retrieved on 22 August 2025.
 16. <https://english.alarabiya.net/News/middle-east/2024/01/11/Turkey-Romania-Bulgaria-ink-deal-to-clear-floating-Black-Sea-mines>, *"Turkey, Romania, Bulgaria ink deal to clear floating Black Sea mines"*, retrieved on 22 August 2025.

17. <http://www.hisutton.com/Ukrainian-USVs-Russo-Ukraine-War.html>, retrieved on 22 August 2025.
18. <http://www.navylookout.com/russian-cruiser-moskva-sunk-in-the-black-sea-assessing-the-implication/>, retrieved on 12 August 2025.
19. [ro.wikipedia.org/wiki/Marea_Neagra](ro.wikipedia.org/wiki/Marea_Neagra), retrieved on 12 August 2025.

MULTINATIONAL MINE COUNTERMEASURES OPERATION IN THE BLACK SEA

Navy Captain Dr. Marian TĂNASE, BEng

Commander of the 39th Diving Center, Constanța

DOI: 10.55535/RMT.2025.3.09

The launch of sea mines anchored in the coastal maritime areas of the Gulf of Odessa, at the beginning of the war between the Russian Federation and Ukraine, led, in the immediate aftermath, to the transformation of the western basin of the Black Sea, an area with important critical infrastructure, into a maritime area at risk from mines.

The appearance of the first active sea mines, drifting from north to south at the end of March 2022, prompted the authorities of the NATO member states bordering the Black Sea to take measures to prevent disasters at sea that could be caused by the explosion of drifting mines upon contact with a ship or a maritime industrial structure.

Since then, the naval forces of Romania, Bulgaria, and Türkiye have begun to conduct their own mine countermeasures operations. The effort required to combat the danger posed by active sea mines drifting in the Black Sea is substantial and must be sustained over a long period of time.

In order to reduce resource consumption and increase the efficiency of their actions, the three allied NATO member states bordering the Black Sea have identified, negotiated, developed, and established a joint solution to the situation: joint actions within a Mine Countermeasures Black Sea Task Group.

Keywords: drifting mines; NAVAREA III; maritime traffic; mine barriers; Black Sea;

INTRODUCTION

One of the major negative effects of the war in the northern Black Sea is *the danger posed by drifting mines*, which significantly affect the freedom and safety of navigation for both civilian and military vessels¹.

Since March 2022, when the first mine was discovered drifting from north to south, each of the three countries, Romania, Bulgaria, and Turkey, organized and began to carry out their own drifting mine countermeasures operation in their area of responsibility with the forces and means at their disposal, while also continuously exchanging information on the situation in the Black Sea.

Since then, the danger of mines in the western Black Sea basin has become permanent, posing a direct threat to the safety of commercial traffic. Military vessels have also limited their presence in the area of responsibility at night, during the execution of specific training activities.

To date, 18 mines originating from minefields laid by belligerents in the Gulf of Odessa have been discovered and neutralized in the area of responsibility of Romania, Bulgaria, and Turkey (Sofia Glob, 2025). In addition, an impressive number of mines have washed up on the beaches of the Ukrainian coast, exploded near the shore, or been discovered and destroyed by the Ukrainian Navy. Of the 18 drifting mines mentioned above, 7 were destroyed by EOD divers from Turkey and 5 by those from Bulgaria. Public reports on drifting sea mines show that the last drifting sea mines were discovered and destroyed by the Turks on March 27, 2025, and by the Bulgarians on May 14, 2024 (ib.).

In Romania's case, EOD combat divers from specialized units belonging to the Romanian Navy destroyed 5 mines, while the 6th exploded upon contact with the hull of the ship "*Lt. Dimitrie Nicolescu*" – 29". The last mine was discovered and destroyed in Romania's area of responsibility on August 13, 2024. The figures made public show that only half of the total number of mines estimated to have been

¹ The letter of the President of Romania addressed to the Chamber of Deputies reads: „*Due to the aggression of the Russian Federation against Ukraine, the threat of drifting mines installed by both states has increased, affecting the safety of navigation and population, as demonstrated by the numerous incidents recorded in the Black Sea, near the borders of Romania.*”. See: Request with no. DSN1/551 of April 3, 2024, addressed to the Chamber of Deputies, <https://www.cdep.ro/co/sedinte.lista?tip=1&an=2024>.

launched in the Gulf of Odessa have been neutralized or destroyed². Thus, the mines still remaining in the minefields in the northwestern Black Sea are a significant source of mine danger on recommended shipping routes and passages, in areas with critical infrastructure, and even along the western coast of the Black Sea.

MANIFESTATION OF THE MINES DANGER IN THE BLACK SEA

On the morning of February 24, 2022, the Russian Federation began its invasion of Ukraine. Immediately, the maritime area in the northwestern basin of the Black Sea, located north of the 45°05' parallel, was declared by international authorities responsible for navigation safety to be a “war risk area” (apud Tănase, 2022, p. 34)³.

Almost a month later, information was released to the public that several hundred sea mines had been launched near the Ukrainian coast in the Gulf of Odessa⁴.

² According to the statement of the commander of the Ukrainian Naval Forces, vice-admiral Oleksiy Neizhpapa, made at the 4th meeting of the „Black Sea Maritime Forum”, held in Naples, Italy, on 15-17 April 2025, the Ukrainian navy discovered and destroyed or recorded the explosion of 200 mines. On the other hand, Romanian open sources mention that, until June 2025, around 130 marine mines, <https://www.navy.ro/comunicat.php?id=925>; apud Tanase, 2023, pp. 22-39 were discovered and destroyed in total.

³ NAVAREA III specified, by notification no. 093/20222, that starting with 24.04.2022, 04:00, the north-west area of the Black Sea, north of the parallel 45°21', is a war risk zone. By the following messages on this subject, the Spanish hydrographic authority maintained the classification of the Gulf of Odessa as a war-risk area but corrected the parallel to the south, which intersects the territorial waters of Romania, at 45°05' (north of the line determined by the following coordinates: ϕ : 45°12'12" N, λ : 2941°06" E; 4511°30" N, λ : 2941°24" E; 4511°30' ' N, λ : 3310°30" E). The notification no. 0124/2022 was in force at the end of September, this canceling the previous one. See NAVAREA III notifications under no. 0093/2022, 0119/2022 and 0124/2022, in the Naval Forces Bulletin/BFN, no. 35/2022; Tanase, 2023, ib.

⁴ On March 18 and 19, 2022, the Russian authorities made public, but also informed the Spanish Hydrographic Office, in charge of NAVAREA III, that Ukraine, in order to strengthen its defense system from the sea, launched chaotic naval mines produced in the first half of the XX century, mines in a poor technical condition and which cannot be controlled at their exit from the dam and when they break away from their anchoring system, being active, they will drift south, influenced by the current of the sea and the wind, and the danger of mines will become a threat to the safety of navigation throughout the western basin of the Black Sea. At that time, the Russians appreciated that the Ukrainians launched in the Gulf of Odessa about 370 mines of the type YAM (town), an anti-desant mine, and of the type YARM (town), anchored river mines. See the text of the press release: <http://www.fsb.ru/fsb/press/message/single.html?id=10439461@fsbMessage.html>.

The hydrographic authorities of Spain, responsible for NAVAREA III, Romania, Bulgaria, and Turkey issued navigational warnings regarding the existence of mines in the Black Sea. Some of these warnings are still in effect today⁵.

On the morning of March 26, 2022, the first sea mine drifting from north to south in the Black Sea was discovered near the entrance to the Bosphorus Strait. This event is extremely important because, in one way or another, the statement issued by the Russians a week earlier has come true. Turkey's announcement that it had discovered and destroyed a (possibly active) mine in its territorial waters made headlines around the world. Both the Black Sea littoral states and the international community realized that what was possible had become a reality.

Immediately, the authorities of the countries bordering the southwestern Black Sea basin took measures to monitor and search for mines in the recommended areas and road and passage systems with the forces and means at their disposal. Since then, ships and helicopters of the naval forces and coast guards of Romania, Bulgaria, and Turkey have been constantly carrying out surveillance and search missions, while also sharing information with each other. Upon discovering the mines, specialized forces from the three NATO member states took action to neutralize/destroy them.

Between March 2022 and August 2025, around 130 sea mines (approximately 30% of the number reported by the Russians regarding mines launched by Ukraine) were neutralized/destroyed in one way or another⁶.

Of these, 6 were discovered and destroyed in Romania's area of responsibility, 5 in Bulgaria's, and 7 in Turkey's, while the rest were discovered and destroyed by the Ukrainians or exploded spontaneously on the Ukrainian coast in or near the Gulf of Odessa.

⁵ On March 19, 2022, the notification of NAVAREA III with no. 0118/2022 took over the information made by the Russian authorities on the discovery of dangerous mines drifting in the area of the NV, west and SV of the Black Sea. The next notification on this topic was the one with no. 0121/2022, stating that drifting marine mines were detected in the same area, without containing the word „possible”. This notice cancelled the previous one. The following notification, under no. 0122/2022, cancelled the one issued earlier and stated that drifting mines are possible in the NV, west and SV of the Black Sea. The port administration of Samsun (province of northern Turkey) issued (19.03.2022/12.15) a NAVTEX message (0279/2022) warning Black Sea merchant ships of the possibility of mine drift and asking them to report any object observed and classified as a possible drift mine. In turn, the Romanian national authority on hydrography, the Maritime Hydrographic Directorate, issued on March 18, 2022, the radionavigation notice no. 12/2022 informing the Romanian authorities and ships in ports and at sea about the existence of the danger of mines in the north-west of the Black Sea and asking them to report any floating object similar to mines. At the beginning of August 2022, the Maritime Hydrographic Directorate issued a new warning, reminding ships sailing in the area of responsibility of Romania that the danger of mines remains high and recommending them to apply the provisions of the notice for seafarers no. 41/4 of the current year (See: RNA no. 60 of 02.08.2022; apud Tănase, 2022).

⁶ Press release no. 8 of 27 January 2023 of the Staff of the Naval Forces (<https://www.navy.ro/comunicat.php?id=680>).



Mission to destroy a marine mine, Eforie marine rayon
(<https://www.navy.ro/eveniment.php?id=1565;15660>)

Public information shows the following breakdown by year and area of incidents related to sea mines that drifted in the Black Sea.

Table 1: Statistics on drifting sea mine events in the Black Sea (author's conception)

Year/Country	Romania	Bulgaria	Turkey	Ukraine	Russia	Georgia	Total
2022	4	1	4	31	0	0	40
2023	1	2	2	46	1	1	53
2024	1	2	0	14	0	0	17
2025	0	0	1	20	0	0	21
Total	6	5	7	111	1	1	131

We can see from the *table 1* above that there was a peak at the end of 2023, and the annual average is 30. The last mines were discovered and neutralized in the areas of responsibility of Bulgaria on May 14, 2024, Romania on August 13, 2024, Turkey on March 27, 2025, and Ukraine on August 10, 2025.

Based on public information, we estimate that there are at least 250 mines still anchored in minefields in the waters of the northwestern Black Sea basin, which must be neutralized through ongoing mine detection and surveillance in offshore areas with critical infrastructure, on passages and routes recommended for maritime traffic and near the coastline on the western coast of the Black Sea, and when a mine clearance operation becomes possible, the involvement of Romania, Bulgaria, and Turkey will also be necessary.

The legal issue of active sea mines that have been found floating adrift, far south of the war zone, has not been discussed for various reasons, although international law provides for specific responsibilities⁷.

Awareness of the risk posed by mines to the safety of navigation in the western Black Sea basin has been raised by the authorities of the riparian countries, the International Maritime Organization, the Spanish hydrographic authority responsible for the NAVAREA III area, companies owning drilling and extraction facilities in the Black Sea, and shipping companies with interests in the Black Sea, was followed by the implementation of specific measures to avoid disasters as far as possible, including:

- *issuing radio warnings to navigators and navigational notices;*
- *restricting certain areas to maritime traffic;*
- *navigating during daylight hours and intensifying visual observation of the maritime space ahead of the ship;*
- *establishing recommended routes and access passages;*
- *conducting research on the recommended routes and passages with ships, aircraft, and drones;*
- *maintaining a high state of readiness, ready for action, of the forces and means for intervention in the event of a drifting mine being discovered (ships and EOD combat diver teams);*
- *negotiating and implementing a format for cooperation and joint action between the three NATO member states bordering the Black Sea: Romania, Bulgaria, and Turkey.*

⁷ No active naval mine shall end up drifting, in international waters or in territorial waters of other states, whether or not neighbouring the war zone, if they have left the mine dam, as they are non-discriminatory weapons. In order to comply with international law, the state which, for one reason or another, resorts to the solution of launching mine dams to strengthen the defence of its maritime coasts must launch mines that become inactive when escaping the dam – to self-destruct or self-inundate. The mines that drifted through the Black Sea in the last year were active mines that did not comply before the launch of the conditions imposed by international law. Consequently, *the person who launched them consciously assumed this fact*. See more: Marian Tănase, *Constraints imposed by international law on naval mine warfare*, in NFB (Buletinul Forțelor Navale), no. 17 (2/2012), pp. 37-49; *Idem*, *Operational and legal considerations on the use of naval mines by the Russian Federation and Ukraine in their confrontation in the Black Sea: From the means of making the A2AD device to the instrument of disinformation and deception*, in NFB no. 35 (2/2022), pp. 22-55.

CHALLENGES IN THE FIGHT AGAINST DRIFTING SEA MINES

The fight against active drifting sea mines, a particular case of mine warfare generated by the need to act in unusual conditions, represents a real challenge for planners, commanders, and the forces at their disposal. Why is it a challenge? This question requires a response in several sentences.

First, the challenge is related to eliminating the danger posed by active sea mines that are drifting, for one reason or another, at a given moment, in a legally confusing situation, where there is no war, but also no crisis, but rather peace, but the situation requires planning and conducting a full-scale war operation to eliminate the mine hazard in the space to be controlled, declared an area of national interest and an area of responsibility for the category of forces – Naval Forces.

Secondly, the entire doctrinal construct relating to mine warfare over the last 50 years has been based on the fact that the dedicated forces and means will act on minefields/barrages launched by the probable enemy to strengthen its defense system from the sea, as part of a defensive operation, which implies the existence of a large number of sea mines, diversified in type, arranged in areas of varying depths, *waiting actively underwater in fixed positions*. The same situation is specific to one's own defense operation, as well as to situations where the probable enemy carries out offensive or maneuvering mining, even if in the latter situation a small number of mines are usually used, which in most cases are of the same type. In most situations, sea mines are weapons that await contact with a ship/submarine or the influence of their physical field.

In almost all navies around the world, the forces and means, as well as the tactical procedures for their use in combat, have been established and designed to act against a *"static enemy"*. Mines are somewhere underwater, and to neutralize/destroy them, their position must be discovered with specific equipment, without endangering the platform and its crew. Mine danger areas are determined based on information about the mining activities carried out by those who launched them. *You know they are there somewhere, but the degree of uncertainty is high.*

Thirdly, the issue of active sea mines drifting in a maritime area has not been sufficiently addressed. It was considered a special case that did not require a special approach in the broader context of naval warfare. Therefore, in combat manuals, references to how to act when a drifting mine is discovered are few and unclear. For situations in which a ship discovers an active naval mine drifting during its action in a district or on recommended routes and passages, specific manuals only stipulate *that the mine should be avoided, fired upon with medium-caliber artillery (greater than or equal to 30 mm), or destroyed with demolition equipment.*

This way of looking at things was not a problem as long as there was no real situation to deal with. However, the current situation in the Black Sea is forcing planners and decision-makers to take a different approach to the fight against drifting mines.

The main operational problem to be solved in mine warfare is *the discovery of the position of mines*/determination of the limits of minefields/mine barriers, both in situations where *mines are waiting underwater in a well-established location*, positioned in the water according to their destination, on the seabed at depths less than or equal to 50 m or at a depth determined by the draft of the ships against which they were launched, as well as *mines that float adrift*, intentionally launched in this mode of operation, mines that have left the dam due to the breaking of the mooring rope or its cutting by the mechanical dredgers of specialized ships during planned actions/operations.

In most situations, a mine that has left the barrier unnoticed or has been deliberately launched adrift moves as an indiscriminate weapon in a direction determined by the combined action of the current, waves, and wind, environmental factors that change depending on hydro meteorological conditions.

Finding a drifting mine is a complex and lengthy process, as there is a high degree of uncertainty. Success in searching for and finding drifting mines in a given maritime area depends on several factors, such as:

- who is conducting the search and what detection equipment they have at their disposal (ships, helicopters, drones, etc.);
- how trained the team in command is in observing floating objects;
- when the search is conducted, day or night;
- what the hydro meteorological conditions are in the search area.

Since there is a large disproportion between the maritime area that needs to be systematically searched and the forces and means available, solutions are needed to ensure an acceptable probability of early detection of drifting mines.

The classic solution is to narrow the search area by establishing a system of recommended passages and routes for navigation and conducting the search with forces and means in the vicinity of these routes according to a set schedule that combines detection capabilities. The effort is great and requires an impressive consumption of resources.

Aerial search with helicopters and drones or other aircraft has the advantage of high speed of movement on established routes, but because the mission is carried out from relatively high altitudes, it is possible that a drifting mine on these routes may be missed.

Systematic search by ship has its advantages and disadvantages. On the one hand, detection is more reliable, but on the other hand, it takes longer and requires more effort.

To detect a drifting mine on board ships, measures have been taken to intensify visual and radio observation on both sides of the ship. As a rule, visual observation is carried out by dedicated observers, who observe the area in front of the ship, on both sides, in a sector from 0 to 30 degrees, with the naked eye and with the aid of binoculars. The observation sector extends to 90 degrees on both sides when dedicated video camera systems or other surveillance or weapon systems are available.

Visual observation is difficult when weather conditions are severe (rough seas, rain, fog, or other phenomena), but especially when performed at night.

Practice has shown that a drifting mine generally has only one-third of its body above water. This means that mines, which are usually painted a dark color, most often black, are only visible at a very short distance from the ship. The distance from which a drifting mine can be observed is significantly reduced when the sea is rough or other hydrometeorological phenomena are present.

An essential condition for protecting the ship and avoiding contact with a drifting naval mine is to detect it at a distance at least equal to the length of the ship. At the same time, in order to ensure that the watch team on the bridge has the necessary time to react and execute the avoidance maneuver, it is imperative that the ship travel at a low speed, between 6 and 12 knots.

As can be seen from the *table 2*, the reaction time for executing the avoidance maneuver is less than one minute when the mine is observed within a distance of 1 cable (180 m).

Table 2: Mine avoidance time depending on detection distance and ship speed.

Discovery distance/ ship speed	6 Nd (3m/s)	8 Nd (4m/s)	10 Nd (5m/s)	12 Nd (6m/s)	Observations
50 ÷ 60 m	15 ÷ 20 s	12 ÷ 15 s	10 ÷ 12 s	8 ÷ 10 s	Length of a minesweeper or sea dredger type vessel
80 ÷ 120 m	26 ÷ 40 s	20 ÷ 30 s	16 ÷ 24 s	13 ÷ 20 s	Length of a minelayer or corvette type vessel
180 ÷ 200 m	60 ÷ 66 s	45 ÷ 50 s	36 ÷ 40 s	30 ÷ 33 s	A frigate-type ship length

Practice has also shown that it is impossible to detect a drifting sea mine with navigation radar, as the mine's radar signature is virtually non-existent.

One solution that can be adopted for the early detection of a drifting mine by a ship performing a dedicated mission or other activities is to equip it with high-performance electro-optical systems that ensure a high probability of detection at a distance that facilitates the safe maneuvering of the ship, both during the day and at night. Eventually, artificial intelligence solutions could be implemented within these systems to train them to detect and identify objects floating at sea, especially in difficult weather conditions.

Another solution is *to ensure air coverage* during the ship's operation in the area or on the recommended routes and paths with dedicated drones for surveillance of the bow area at a safe distance and from low altitudes. The number of drones available on board the ship must ensure that the surveillance cycle can be resumed without interruption. The performance of the drone's video camera must ensure the detection of small objects floating adrift, both during the day and at night, and if possible, in foggy conditions. On the one hand, the drone used must have sufficient autonomy, and on the other hand, the limits of the drone's flight conditions must be at least the same as the ship's navigation limits.

The early detection of a drifting mine in the bow area of the ship by observers or with the aid of on-board electro-optical systems requires, as a first measure, avoiding it and bringing the ship into a position that ensures the safe stationing of the ship and keeps the mine within visual range. This should be followed by reporting the position of the discovered mine, keeping it within sight, and, if possible, carrying out destruction procedures.

A mine discovered by a ship can be destroyed by the dedicated destruction team on board, consisting of EOD combat divers. However, not in all situations do ships conducting mine countermeasures have such specialized teams on board. This requires monitoring the mine for a period of time equal to that required to deploy such a team to the area, with another ship or helicopter. At the same time, the process of monitoring a drifting mine by the ship that discovered it is not at all simple, especially if the hydro meteorological conditions are not favorable.

The procedure for avoiding a discovered drifting mine is the classic procedure for avoiding any dangerous floating object, except for ships. The avoidance maneuver is performed, on one side or the other, at a distance of at least 50 m or at least equal to the length of the ship. If there is wind, the maneuver is performed so that the mine is left on the windward side, at a safe distance.

The maneuver is considered complete when the mine has been left astern and the ship has returned to its previous course, from where it continues on its way, takes its place in formation, if it was previously sailing in a specific formation, it takes up a surveillance position or a position for lowering the demolition team's boat, which will carry out the mine intervention, a position that will keep the mine within visual range and ensure that the ship remains at a safe distance from the mine.

The destruction of a drifting sea mine by a demolition team is a classic procedure. It has been applied both in the case of the accidental discovery of a drifting mine, when time allowed, and in the case of mines that have been dredged and have not self-destructed. The emergence and development of the EOD combat diver specialty has made it possible to intervene on a drifting mine to neutralize/destroy it with specially trained teams, rather than with teams made up of ship crew members trained in underwater weapons. This procedure applies when the sea state is a maximum of 2.

Mine warfare manuals provided and still provide for a procedure for neutralizing mines from a distance with medium-caliber artillery installations by shooting. The purpose of this procedure was justified by the fact that, in wartime, ships generally sail in formation, and the mission they have to carry out is more important than the need to destroy a drifting mine discovered in the vicinity of the formation, there is not enough time to use the destruction team, or the sea state does not allow the destruction team to intervene, and firing the ship's artillery, which is always ready to fire, would ensure that the mine is hit and sunk in a short time. Although there are still specific procedures for firing weapons larger than 20 mm at targets that mimic a drifting mine, and training is conducted in this regard, practice has shown that the probability of hitting a mine whose body floats on the surface is only 1/3, which results in a large and unnecessary consumption of ammunition. In the absence of an emergency situation, it is better to avoid adopting this ineffective solution.

In many situations, it is possible that neither of the two procedures can be applied nor have been applied unsuccessfully, which forces the postponement of the moment when the mine can be neutralized or destroyed. In these situations, knowing the position of the mine for a longer period of time (e.g., at least 24 hours) is essential for successfully eliminating the danger posed by the mine. How can such a problem be solved, especially in difficult weather and sea conditions, when the ship cannot remain in the vicinity of the mine and is forced to retreat to port?

One solution that can be adopted is *to mark the mine* with a device that tracks its position using the GPS system. To do this, you need to approach the mine and place the GPS tracking device on it, which will remain on the mine for a long time (until the battery life expires). This device is attached to a net that is launched onto the mine by a drone controlled from the ship. The net remains on the mine by means of a device that tightens its edges around the mine. This is the operating principle of the *prostovol*, a classic fishing tool. In this way, by periodically transmitting the position of the mine by the device remaining on the mine, a drifting mine can be tracked from the ship or from another operations center, especially in bad weather or at night.

The fight against active drifting sea mines should no longer be seen as a rare occurrence in mine warfare, but requires a special approach, both theoretical and practical. It is imperative to equip combat ships with high-performance observation and search systems, as well as to find the most effective and safe solutions for eliminating/managing the mine hazard generated by drifting sea mines.

In the fight against active drifting sea mines, it is very important to detect them early, but also to intervene as quickly as possible to destroy them or keep them under continuous observation until specialized forces can intervene.

Systematic naval reconnaissance of recommended passages and routes, as well as areas with critical infrastructure, is an important part of an operation to combat drifting mines. It requires a significant amount of forces to be present at sea and a long period of action.

While each Black Sea littoral state is responsible for its own territorial sea and each has its own interagency mine countermeasures operation in place, for the high seas, a mine countermeasures operation undertaken by the littoral members of the North Atlantic Alliance is an effective and important solution, a component of cooperation, interoperability, and unity on NATO's eastern flank, given the deteriorating and volatile security environment in the wider Black Sea area.

MINESWEEPING OPERATION IN THE BLACK SEA

Given the permanent deterioration of the security environment in the Black Sea, the three NATO allies bordering the Black Sea sought a common solution to respond to an important real problem – drifting mines.

Towards the end of 2023, Turkey invited Romania and Bulgaria to form a *joint mine countermeasures task force* as a common measure to ensure the security and safety of navigation in the Black Sea.



Romanian Minister of Defense Angel Tîlvăr, Turkish Minister of Defense Yasar Guler, and Bulgarian Deputy Minister of Defense Atanas Zaprianov at the ceremony in Istanbul, Daily News, 2024

Following their positive response, on January 11, 2024, the Ministers of National Defense of Bulgaria, Romania, and Turkey, meeting in Istanbul, signed, during a ceremony, the *“Memorandum of Understanding on the Establishment of the Task Group for Combating Sea Mines in the Black Sea – MCM Black Sea TG”*⁸. This extremely important document forms the basis for the deployment of the *multinational mine countermeasures operation in the Black Sea*, starting on July 1, 2024. This political-military action was not only a first for the NATO member states bordering the Black Sea, but also the most important political-military action relating to the security situation in the Black Sea region since Bulgaria and Romania became members of the North Atlantic Alliance (2004).

Furthermore, the MCM Black Sea Task Group is of particular strategic importance because:

- the security of the Black Sea region is an absolute priority for the three coastal countries;
- the three allies have demonstrated to the Euro-Atlantic community that they are united in their common commitment to combat the danger posed by sea mines drifting in the Black Sea from north to south;

⁸ Press release no. 6 of 11 January 2024 of M.Ap.N., <https://www.mapn.ro/>.

- the foundations have been laid for a security arrangement open to NATO partners bordering the Black Sea and other allied states, as well as to permanent NATO structures such as permanent naval groups such as SNMCMG2.
- The three allies expressed their confidence that the measures taken would contribute to the development of cooperation and increased interoperability of their naval forces, but not only that, by participating significantly in ensuring the security of the Black Sea and the entire Euro-Atlantic region.
- The joint mine countermeasures operation in the Black Sea has been added to other initiatives that play an important role in maintaining regional security, such as *air policing*⁹.

In regard to Romania, following the president's request, on April 22, 2024, Parliament approved by a decision the participation of the Romanian Naval Forces in the operations carried out within the Operational Group for Combating Sea Mines in the Black Sea - MCM BLACK SEA, which came into force the following day, upon its publication in the Official Gazette¹⁰. Based on the Memorandum and national approvals, the naval staffs of Bulgaria, Romania, and Turkey negotiated and drafted the documents underlying the joint mine countermeasures operation in the high seas area of the western Black Sea basin.

The operational structure of MCM Black Sea consists of the Black Sea Mine Countermeasures Committee (*MCM Black Sea Committee*), made up of the chiefs of the navies of the participating countries, and the Black Sea Mine Countermeasures Task Group (*MCM Black Sea Task Group*).

The *MCM Black Sea TG* consists of the group commander (CTG) with his staff, the ship unit commander (CTU) with his staff, a command ship, and at least three ships specialized in mine countermeasures, such as mine hunters or sea minesweepers.

The main missions of the MCM Black Sea TG are:

- ensuring the safety of navigation in the Black Sea;
- strengthening the allied deterrence posture;
- contributing to the defense of the southern flank.

The MCM Black Sea TG has a rotating command every six months and two planned activations, each lasting 15 days.

⁹ For Romania, „the creation of a task force is both a way to develop regional cooperation with its rival allies, and an opportunity to increase the participation of NATO and non-riveran allies in ensuring the security of the Black Sea”. See: Decision no. 9 of 22 April 2024 published in the Official Gazette, Part I, no. 377, April 23, 2024.

¹⁰ *Ib.*, Decision no. 9 of 22 April 2024 published in the Official Gazette, *loc. cit.*

During a rotation, one of the countries is responsible for providing the command positions and the group's command ship. Command of the group is held by an officer with a minimum rank of commander. This is handed over/received in the presence of the *MCM Black Sea Committee*, during a dedicated ceremony.

Within the ship group, each country provides at least one ship specialized in mine warfare, and the country responsible for the rotation allocates a command ship on board which the ship group commander (CTU) and his staff embark.

The functions within the CTG and CTU staffs are allocated to each country based on an algorithm agreed upon in the operation documents.

As regards Romania, participation has been approved with a force package consisting of a military vessel with MCM capabilities and an EOD team on board, with a crew of up to 85 military personnel and staff (up to 6 military personnel).

The periodic reconfiguration of Romania's contribution to MCM BS TG, within the limits of the initially established force package, is periodically approved by the Ministry of National Defense, depending on operational needs and the evolution of the operation¹¹.

On July 1, 2024, the first meeting of the Black Sea Mine Action Committee was held in Istanbul, followed by the assumption of command of the group (MCM BS TG) by a Turkish admiral, Rear Admiral Selcuk Akari, in the presence of the admirals, heads of the navies of Bulgaria, Romania, and Turkey. For the first rotation, the MCM BS TG consisted of the following ships:

- Turkey: the logistics support ship "*GÜNGÖR DURMUŞ*" (A-574); the minesweeper "*AKÇAY*" (M-270);
- Romania: the sea minesweeper "*Sublocotenent Alexandru AXENTE*" (DM-30);
- Bulgaria: minesweeper "*STRUMA*" (M-33)¹².

During this first rotation, MCM BS TG was active from July 2 to 16, 2024, September 19 to 29, 2024, and November 1 to 13, 2024. For the first activation, from July 2 to 4, 2024, the ships joined the group in the Turkish port of Umuryeri (Istanbul), where they underwent their first joint training under the conditions set out in the basic documents resulting from the Memorandum, and carried out a joint march to the Bulgarian port of Burgas from July 4 to 6, during which joint mine countermeasures were carried out. MCM BS TG participated for the first time in a multinational exercise organized and conducted in the Black Sea, the "*BREEZE 24*" exercise.

¹¹ *Ib.*

¹² Press release no. 53 of 1 July 2024 of SMFN, <https://www.navy.ro/>.



Left: MCM BS group vessels docked in Umuryeri port
Right: Chiefs of the General Staff of the Naval Forces of Romania, Turkey, and Bulgaria
(<https://www.navy.ro/eveniment.php?id=1998>)

After several days of stationing in Burgas, MCM BS TG conducted mine countermeasures on recommended passages and routes in the area of responsibility of the Bulgarian Navy, in accordance with the exercise documents, between July 8 and 12. After completing its mission at sea and restoring its combat capability in the port of Burgas, MCM BS TG carried out activities specific to maintaining the safety of navigation routes during the voyage from Burgas to Constanța (July 14-15), and between July 15 and 17, 2024, the group's ships docked for the first time in Constanța, where their combat capability was restored.

During their visit to the Port of Constanța, representatives of the group were received at the “Vice Admiral Vasile Urseanu” Fleet Command and at local public institutions in the Municipality of Constanța, and participated in a media event promoting the missions of the operational group for combating sea mines in the Black Sea¹³.

The first activation ended on July 16, 2024, at midnight, and the Turkish and Bulgarian ships left the port of Constanța the following morning.

During the two weeks they operated together, the ships and their crews worked to increase their level of interoperability and rapid response capability.

The MCM BS group ships met in the port of Burgas on September 19, 2024, to begin their second activation. Until September 29, 2024, MCM BS TG conducted mine countermeasures during transit from Burgas to Eregli (September 22-24, 2024), during participation in the multinational exercise “NUSRET 24” organized by the Turkish Naval Forces in the areas near the port of Eregli, and during

¹³ Naval Forces Staff, Press release no. 98, 14.11.2024.

the redeployment march to their permanent stations¹⁴. During the exercise, EOD divers aboard the ships worked together to neutralize drifting mine simulators.

In its third activation, from November 1 to 13, 2024, MCM BS TG participated in the multinational exercise “POSEIDON 24” organized by the Bulgarian Navy in the port of Burgas and in the maritime areas nearby (November 4-9, 2024).

The Romanian Navy participated in the third activation of MCM BS TG with the maritime minesweeper “*Lieutenant Dimitrie NICOLESCU (DM-29)*”.

During the “POSEIDON 24” exercise, the mine countermeasures group carried out specific missions to search for, detect, and identify historical and exercise mines, both anchored and bottom-laid.

After leaving the port of Burgas, during the transit to the port of Constanța, the ships of the Black Sea mine countermeasures task force conducted drift mine search on the recommended routes in the areas of responsibility of the Bulgarian and Romanian navies.

From November 12 to 14, 2024, the second stopover of the MCM BS TG took place in the military port of Constanța¹⁵. Bulgaria was the country responsible for the second rotation. On January 15, 2025, the MCM Black Sea Committee meeting and the ceremony for the change of command of the Black Sea Mine Countermeasures Task Group took place in Varna.

Command of the group was taken over by Captain I (Commander) Pavlin Petkov, and the flagship was the auxiliary ship “*Captain I Dimitar Dobrev*”.

This time, all three ships specialized in mine warfare were mine hunters. The Bulgarian Navy continued to assign the “*STRUMA*” (M-33), and the Turkish Navy assigned another ship, the minesweeper “*AKCAKOCA*” (M-268). The Romanian Navy also provided the MCM BS TG with a minesweeper. Romania’s efforts to acquire operational mine countermeasure capabilities came to fruition with the commissioning of the first minesweeper from a package of two purchased from the United Kingdom. The minesweeper “*Sublocotenent Ion GHICULESCU (M-270)*” received the national flag on September 27, 2023, entering the service of the Romanian Naval Forces, and arrived in the country on December 19, 2023¹⁶.

After undergoing a process of operationalization, the mine hunter “*GHICULESCU*” was ready for mission at the beginning of 2025 to be made available to the Black

¹⁴ Maritime dragon “*Sub-lieutenant Alexandru AXENTE*” (DM-30) left the port of Eregli on 28 September 2024 and entered the port of Constanta the next day.

¹⁵ Naval Forces Staff, Press release no. 53/01.07.2024.

¹⁶ Defence Staff, Press release no. 156, 18.12.2023.



MCM Black Sea Committee, January 15, 2025, Varna

Sea mine countermeasures task force. Thus, Romania's contribution to maintaining the safety of navigation in the Black Sea has been taken to a higher level thanks to the specific operational capabilities of minesweepers.

At the MCM Black Sea Committee meeting in Varna, the activity of the MCM BS group in the first six months was analyzed, conclusions were drawn, and some amendments were made to the planning documents.

Under Bulgarian command, the MCM BS TG was activated twice as planned.

The first activation in 2025, the fourth for the group, took place between April 3 and 17, 2025. The group's ships gathered on April 2, 2025, in the Bulgarian port of Varna, and on April 5, they arrived in the port of Constanța to participate in the multinational exercise "SEA SHIELD 25", organized by the Romanian Naval Forces, between April 5 and 11, 2025¹⁷.

¹⁷ Naval Forces Staff, Press release no. 22, 02.04.2025.

During the exercise, for three days (April 8-10, 2025), the three minesweepers carried out specific missions to search for historical bottom mines and anchored exercise mines.

MCM BS TG continued its mine surveillance and search mission on the recommended routes and roads between the parallels of the ports of Constanța and Varna (April 12-16, 2025). After restoring their combat capability, the minesweepers “AKCAKOCA” (M-268) and “*Second Lieutenant Ion GHICULESCU*” (M-270) departed for their permanent stations.

The second activation of the MCM BS group took place between June 11 and June 26, 2025. It began in the Bulgarian port of Burgas and ended in Istanbul, Turkey. During this period, the ships of the MCM BS TG also stationed in Constanța and participated in the multinational exercise “*EP MCM DIVE-25*” organized by the Romanian Naval Forces.

The ships of the MCM BS TG gathered in the port of Burgas (June 10, 2025). After participating in the opening ceremony of the fifth activation (June 11, 2025), the MCM BS TG was present at sea for two days, conducting mine countermeasures and surveillance of important maritime communication routes between Burgas and Constanța.

The participation of the MCM BS TG in the multinational exercise “*EP MCM DIVE-25*”, organized by the Romanian Naval Forces between June 15 and 19, 2025, provided the ships, crews, and EOD divers with the opportunity to jointly perform specific procedures for neutralizing drifting mines, as well as to exchange experiences in performing specific missions among participants.

The search for drifting mines, an essential task of the MCM BS group, was also carried out during the transit from Constanța to Umuryeri (Istanbul) between June 22 and 24, 2025.

Starting on July 9, 2025, Romania is responsible for commanding the Black Sea Mine Countermeasures Task Group (MCM BS TG).

For the third rotation of the MCM BS TG, the Naval Forces General Staff provided the mine countermeasures vessel “*Vice Admiral Constantin BĂLESCU – 274*” as the command ship of the group of ships and the mine countermeasures vessel “*Second Lieutenant Ion GHICULESCU*” (M-270). They were joined by the minesweepers “*STRUMA*” (Bulgaria) and “*AMASRA*” (Turkey). The foreign ships arrived in Constanța on July 8 for integration and the handover ceremony of the group’s command.



MCM Black Sea Committee, July 9, 2025, Constanța

During the meeting of the Black Sea Mine Countermeasures Committee (MCM Black Sea Committee) held on July 9, 2025, the Chiefs of Staff of the Naval Forces of Romania, Bulgaria, and Turkey analyzed the group's activity under Bulgarian command, signed the official declaration of command takeover for a period of six months, and approved the organization and planning documents for the next six months, as well as some specific procedures necessary to strengthen the joint action of the forces made available within the group¹⁸.

On the same date, in the Port of Constanța, at the passenger terminal, the handover ceremony of the MCM Black Sea Task Group command took place. Captain I Pavlin Petkov of the Bulgarian Navy handed over the command to Commander Marian Tănase of the Romanian Navy. The ceremony was attended by the Minister of National Defense, the Chief of Defense Staff, the Chiefs of Staff of the Naval Forces of Romania, Bulgaria, and Turkey, ambassadors, military attachés, representatives of local authorities, commanders of ships participating in the 2nd and 3rd rotations, commanders of units and large units of the Romanian Naval Forces, and other guests.

¹⁸ Defence Staff, Press release no. 62, 07.07.2025.



Delivery-receipt of order MCM BS TG, July 9, 2025, Constanța

During this rotation, the ships of the MCM Black Sea Task Group participated in the first planned activation (July 2025) in the multinational exercise “BREEZE” organized by the Bulgarian Naval Forces, and during the second activation (October 2025) they will participate in the multinational exercise “POSEIDON” organized by the Romanian Naval Forces, an exercise focused on mine warfare.

During the first planned activation (the 6th activation), July 10-24, 2025, the ships of the MCM Black Sea Task Group participated in the multinational exercise “BREEZE” from July 11 to 20. During the transit from Constanța to Varna, the sea training period within the multinational exercise “BREEZE”, and the transit from Varna to Umuryeri, the MCM Black Sea Task Group conducted drift mine countermeasure research with its ships on recommended routes and passages in the areas of responsibility of the three navies.

As part of its seventh planned activation in October 2025, the MCM Black Sea Task Group will be present in Constanța to participate in the multinational exercise “POSEIDON” organized by the Romanian Naval Forces.

In the first 15 months since its establishment, the MCM Black Sea Task Group has demonstrated the willingness of the three Black Sea allied countries to participate in the joint effort to combat the mine threat in the Black Sea.

The main purpose of the Task Group is to maintain the safety of maritime traffic in the Black Sea by conducting surveillance, reconnaissance, and neutralization of sea mines, as well as related search and rescue operations at sea.

Mine countermeasures on recommended routes and passages in the territorial waters of MCM BS participating countries, carried out by the group’s specialized vessels, are a core mission during multinational exercises, but also during voyages from one port to another.

Typically, during an activation, the group’s specialized mine countermeasure vessels travel around 1,000 nautical miles, are present at sea for around 300 hours, cover an area of around 400 square nautical miles searched for drifting mines, and search an area of several tens of square nautical miles for bottom mines.

This joint effort contributes continuously to the integration of forces, facilitates the real exchange of experience, and encourages the navies of the three states to improve the level of interoperability of the capabilities made available to the MCM BS Group, which together contribute to a better understanding of the maritime situation in the Black Sea by both the three states and NATO.

Improving joint action procedures and those related to command and control in an international environment, combat readiness, strategic communication, and mutual support are important factors in increasing the operational efficiency of the MCM Black Sea Task Group. The observation has been made from one activation to another

CONCLUSIONS

Since the adoption of the Hague Convention (1907), the operational use of sea mines has been regulated by international law, but this has not guaranteed, nor will it guarantee in the future, full compliance with these rules by the belligerents.

The lessons learned from maritime operations in previous conflicts oblige military planners not to remove from the list of analysis assumptions for taking specific measures or planning the actions/operations necessary to ensure maritime

security in their area of responsibility the fact that a state or non-state actor may not comply with the legal norms of maritime law, both general and specific to the use of sea mines, when it has divergent interests with its neighbors or with the international community. One of the important consequences with a major impact on the safety of commercial maritime traffic, the protection of critical infrastructure, and the marine environment, both in territorial waters and on the high seas, is the use of mines.

One of the important consequences with a major impact on the safety of commercial maritime traffic, the protection of critical infrastructure and the marine environment, both in territorial waters and on the high seas, is the danger posed by sea mines detached from minefields/mine barriers launched for operational purposes or sea mines that have been deliberately launched without anchors, which drift in directions determined by the combined action of currents, waves, and winds passing through areas far from the actual conflict/war zone.

A telling example in this regard is the war between the Russian Federation and Ukraine, which began on February 24, 2022, and continues today.

The war between Russia and Ukraine has created a situation in the Black Sea that was not anticipated 10 years ago. Although it should not have happened, the use of conventional sea mines took many people by surprise.

An important consequence of the use of sea mines in the northwestern basin of the Black Sea is the manifestation of the danger of mines in maritime areas located at a considerable distance from the war zone, due to the presence of active sea mines adrift.

This poses a real danger to both maritime traffic safety and the integrity of critical infrastructure, but also a flagrant violation of international maritime law, as it requires that a sea mine that has left the barrier for a specific reason must self-destruct or self-inundate.

The launch of the *“special military operation”* in Ukraine by the Russian Federation constituted a justified, operational, and legal reason for Ukraine to use, among other means, the sea mines in its navy’s depots to establish an A2AD zone in its territorial sea.

In the case of the Russian Federation, it can be argued that if it had any operationally justified reasons for launching sea mines in areas near Ukraine’s territorial sea, it did so without complying with international maritime law.

On the other hand, given the type of mines discovered floating adrift south of parallel 45°05' and that they were active, it follows that whichever party launched them, anchored in a barrage or intentionally adrift, violated the rules imposed by the Hague Convention. Determining responsibility for their deployment will be a matter to be resolved according to the political decisions taken by the two states involved, the Black Sea littoral states affected by the mine hazard, the states under whose flags the damaged ships were sailing, and even by other members of the international community.

If we assume that the mine that appeared in March 2022 near the coast of Turkey was a mine that came out of a dam launched in the Gulf of Odessa by one of the parties, then it follows that it floated through the Black Sea in a general north-south direction for several days without being detected by any ship or other surveillance system. At that time, commercial shipping in the Black Sea was extremely limited due to the ban on entering Ukrainian ports and the danger in the war zone.

During the three and a half years of war in the northwestern Black Sea, 17 other sea mines followed the same route as the one discovered in March 2022, and around 110 appeared on the beaches of Odessa Bay, were destroyed, or exploded upon colliding with various obstacles.

If we take into account the information on the number of mines launched near Ukrainian ports, provided by the Russian secret service, around 370, and the fact that around 30% of these have left the barrier within 3 years, we estimate that in the coming period other sea mines will be discovered floating adrift as a result of their detachment from the mine barriers due to hydro meteorological conditions and the impact of time on underwater mine systems.

The use of sea mines during an international crisis in a maritime area between two neighboring states, as is the case with the conflict between Russia and Ukraine, obliges the international community to intervene to control, reduce, and/or eliminate the danger of mines in the region.

As we have already argued and as practice shows, the effort required to successfully conduct a mine clearance operation against drifting mines is considerable and consumes significant resources.

The fight against active naval mines drifting in the Black Sea is a full-fledged war operation and, as a result, must be approached, recognized, and treated as such,

even though none of the NATO member states with significant territory in the Black Sea basin are at war.

Romania's area of responsibility, more so than that of the other two NATO member countries, Turkey and Bulgaria, is exposed to the danger of mines, given its position in the Black Sea, close to the war zone.

On the other hand, none of these countries can undertake such an operation on its own, but each is obliged, in one form or another, to conduct its own mine warfare operation.

The fight against sea mines in the Black Sea to eliminate the mine threat south of the Russian-Ukrainian conflict zone requires the planning and execution of a real combat mission in peacetime conditions.

The fact that the three neighboring allies in the Black Sea, Romania, Bulgaria, and Turkey, have managed to establish the legal framework for conducting a joint operation against active sea mines drifting in the Black Sea, to form a group of ships specialized in mine warfare, with relational command and planned periodic activations, and to periodically carry out mine search missions on recommended routes and passages in the areas of responsibility of the three states is a diplomatic and military success that expresses the political will of Romania, Bulgaria, and Turkey to work together to ensure the safety of maritime traffic and the protection of critical infrastructure in the western Black Sea basin.

Since the beginning of July 2025, for a period of five months, the MCM Black Sea Task Group has been under the command of a Romanian officer. The ships made available to the group commander by the three signatory states are minesweepers, ships specialized in mine countermeasures. They have important specific operational capabilities, and their crews carry out their mission within the group based on common operational procedures, practiced during regular training.

The MCM Black Sea Task Group has the necessary capabilities and sufficient combat experience to successfully carry out its assigned missions.

BIBLIOGRAPHICAL RESOURCES:

1. Daily News (2024), <https://www.hurriyetdailynews.com/turkiye-bulgaria-romania-sign-black-sea-demining-deal-189593>, retrieved on 22 August 2025.
2. Hotărârea nr. 9 din 22 aprilie 2024, in *Monitorul Oficial*, Part I, no. 377, 23 April 2024.
3. Sofia Glob (2025), <https://sofiaglobe.com/2025/02/04/bulgarian-navy-chief-18-mines-destroyed-in-black-sea-since-start-of-russias-war-on-ukraine/>, retrieved on 22 August 2025.

4. Solicitarea nr. DSN1/551/ 3 April 2024, adresată Camerei Deputaților, <https://www.cdep.ro/co/sedinte.lista?tip=1&an=2024>, retrieved on 12 august 2025.
5. Tănase, M. (2023). *Lupta contra minelor navale aflate în derivă: considerații operaționale privind adoptarea viitoarelor soluții pentru restabilirea statutului de „ape sigure” al Mării Negre*, in *Buletinul Forțelor Navale*, no. 36, pp. 22-39.
6. <https://www.navy.ro/comunicat.php?id=925>, retrieved on 12 August 2025.
7. <http://www.fsb.ru/fsb/press/message/single.htm%21id%3D10439461%40fsbMessage.html>, retrieved on 22 August 2025.

COGNITIVE WARFARE – A NEW OPERATIONAL DOMAIN –

Colonel Dr. Marian HOGEA

“Nicolae Bălcescu” Land Forces Academy, Sibiu

DOI: 10.55535/RMT.2025.3.10

Cognitive warfare is one of the most recent and complex forms of conflict in the global environment, in which the human mind becomes both a target and a strategic tool. The cognitive dimension, considered an emerging operational domain distinct from traditional ones – land, sea, air, space, and cyberspace, focuses on influencing the perceptions, emotions, and decision-making processes of individuals and communities, constituting an essential strategic vector in the dynamics of contemporary international relations. A comparative analysis of the strategies used by NATO, Russia, and China illustrates that cognitive warfare has become a central tool in the dispute between the great powers, with direct effects on the stability of the world order.

Keywords: cognitive warfare; global security; strategic influence; strategic manipulation; psychological influence;

INTRODUCTION

In the current context of globalization, marked by technological progress and information globalization, *cognitive warfare* stands out as a new battlefield. Unlike traditional domains – land, sea, air, space, and cyberspace –, it seeks to influence the perceptions, emotions, and decision-making processes of individuals and communities, thus representing a particularly relevant strategic tool in confrontations between major powers.

The cognitive dimension of global confrontations highlights the differences between information and psychological warfare, as well as its implications for global security and social cohesion. Campaigns to influence democratic processes illustrate the concrete effects of cognitive warfare, while ethical and legal analysis underscores the need to develop resilience policies and appropriate international regulatory frameworks

The term “*cognitive*” comes from the Latin *cognoscere* (“to know”, “to understand”), derived from the root *gnoscere* (“to learn”, “to know”). In its modern sense, it was established with the development of cognitive psychology and neuroscience, becoming a central concept for describing mental actions.

In psychology, the term gained visibility in the second half of the 20th century as a reaction to the limitations of *behaviourism* (a psychological current focused on the study of behaviour, of the external stimulus-response relationship), which facilitated the analysis of observable behaviour, excluding internal processes. In the period 1950–1960, the cognitive revolution (<https://brainly.ro/tema/6593720,b2025>) emerged, proposing an approach to the mind as an information processing system, analogous to the functioning of computers. (Miller, 1956, pp. 81-97). Ulric Neisser established the terminology in his work *Cognitive Psychology*, where he defined cognitive psychology as the study of the processes by which information is acquired, stored, and used (Neisser, 1967, pp. 3-20).

Thus, the term “*cognitive*” now refers both to the fundamental processes of cognition – perception, reasoning, attention, memory, decision-making – and to the conceptual framework that integrates the interaction between mind, brain, and environment. This evolution explains the expansion of the term beyond psychology and neuroscience to fields such as social sciences, communication theory, and security studies, where “*cognitive*” is analysed in relation to the influence, manipulation, and control of information in geopolitical and strategic contexts.

In his analysis entitled *“Cognitive Warfare: A Conceptual Analysis of NATO’s Cognitive Warfare Concept”*, Christoph Deppe defines cognitive warfare as an emerging form of conflict focused on influencing and manipulating the perception and decision-making processes of individuals or groups of individuals in order to gain a strategic advantage. (Deppe, Schall, 2024). Cognitive warfare systematically exploits scientific knowledge about the cognitive functioning of the human mind to influence and manipulate the perceptions, decision-making processes, and behaviours of individuals and communities. It redefines the human mind as an operational domain, using psychological operations, disinformation, propaganda, social engineering, and digital technologies to achieve strategic and tactical objectives without resorting to conventional force. This emerging form of conflict seeks to gradually erode the collective will and resilience of adversaries. Thus, cognitive warfare directly targets the mental and cognitive processes of actors, influencing how they perceive, interpret, and process information, as well as their decision-making processes.

In modern conflicts, the terms cognitive warfare, information warfare, psychological warfare, ideological warfare, economic warfare, technological warfare, religious warfare, diplomatic warfare, and cyber operations are often used interchangeably, but each represents a distinct dimension of the struggle for influence and control.

In the post-Cold War context, the evolution of armed conflicts has highlighted a diversification of tactics and procedures, accompanied by a doctrinal reconfiguration that has shifted the emphasis from kinetic to non-kinetic means, subsumed under the neo-military paradigm (Hoffman, 2007, pp. 6-17).

Table 1: Comparisons between kinetic tactics and non-kinetic (neo-military) tactics

Dimension	Kinetic (traditional)	Non-kinetic (neo-military)
Main objective	Physical destruction of the adversary’s force and infrastructure	Influencing the adversary’s perceptions, will and decision-making capacity
Means	Conventional armament, land, air, naval, space operations	Information, psychology, economy, cyberspace, culture, law
Method of action	Direct strikes, classic military confrontation	Manipulation, disinformation, indirect pressure, cyber attacks
Immediate effect	Human losses, material destruction	Confusion, demoralization, social and political destabilization

Dimension	Kinetic (traditional)	Non-kinetic (neo-military)
Attribution	Easy to identify (it is known who is attacking)	Often ambiguous or denied (“under /below the threshold” operations, deniable)
Duration of impact	Short or medium term (until capacity is reconstituted)	Long term (modifies mentalities, social relations, economic dependencies)
Examples	Military invasions, bombings, conventional battles	Information warfare, psychological warfare, cyber, economic, cognitive warfare

Cognitive warfare refers to actions aimed at influencing the mental processes of individuals or groups, including perception, information assessment, and decision-making (Claverie, du Cluzel, 2023, pp. 1-4). Its central objective is not only to manipulate informational content, but to shape the way it is processed, thereby affecting the interpretation of reality and the ability to make rational decisions. Relevant examples include the use of structured information flows, subtle disinformation, or artificial intelligence algorithms to shape public opinion and indirectly influence social behaviour. Therefore, cognitive warfare targets the human mind and internal information processing mechanisms.

Information warfare consists of “the collection, manipulation, and dissemination of information to influence the perceptions and behaviours of the adversary” (Joint Chiefs of Staff, 2004, pp. 21–30). Unlike cognitive warfare, the focus is on the content of messages and communication channels rather than on internal cognitive processing. Examples include propaganda, fake news, digital disinformation campaigns, or the interception and modification of communications. Thus, information warfare aims to control the flow of information and shape perceptions of external reality.

Psychological warfare aims to influence emotions, attitudes, and behaviours through direct or indirect psychological techniques. Unlike cognitive warfare, which targets the structures and mechanisms of thought, psychological warfare focuses on motivations and emotional reactions (Neacșu, 2004, pp. 21-30). Examples include psychological terror campaigns, demoralizing messages to opposing troops, or inducing fear and uncertainty to undermine group cohesion. This type of warfare has older historical roots and is still relevant in traditional influence operations.

Ideological warfare aims to promote and impose a set of values, beliefs, or doctrines on a social group or nation. The main objective is to shape collective

beliefs and cultural norms, influencing long-term behaviours (Dobrinescu, 2017, pp. 33-44). Unlike cognitive warfare, which targets individuals, ideological warfare focuses on communities and cultural structures. Examples include promoting political doctrines, supporting social movements to destabilize the adversary, or transnational propaganda campaigns.

Economic warfare involves the use of financial, commercial, and industrial resources to diminish an adversary's ability to act strategically. Actions are aimed at disrupting production, access to resources, or economic stability (Popa, 2018, pp. 45-53). Examples include economic sanctions, trade blockades, manipulation of financial markets, or attacks on critical infrastructure. Unlike cognitive or information warfare, the effects are material and quantifiable, with indirect repercussions on social perceptions and behaviours.

Technological warfare focuses on the development and application of advanced technologies to achieve strategic or tactical superiority. Objectives include either improving one's own capabilities or sabotaging those of the adversary (Zodian, 2019, pp. 7-18). Examples include the development of hypersonic weapons, autonomous drones, advanced surveillance systems, or encryption and automated disinformation technologies. Unlike cyber operations, technological warfare includes both hardware and software components integrated into complex systems

Religious warfare uses religious beliefs and institutions to mobilize mass support, generate divisions, or weaken the adversary. Unlike ideological warfare, the emphasis is on spiritual values and sacred norms, not political or social doctrines (Cîrstocea, 2016, pp. 55-67). Examples include tensions or confrontations between different religious groups, religious radicalization, or the use of religion to legitimize a conflict. The impact is felt at the social and cultural level, influencing the cohesion and stability of communities.

Diplomatic warfare involves the use of international relations, negotiations, and political pressure to gain strategic advantages without resorting to direct force. The objective is to influence the behaviour of states or international organizations through alliances, isolation of the adversary, or manipulation of external opinions (Mouslim, 2022, pp. 423-445). Examples include international sanctions, lobbying in multilateral organizations, strategic bilateral negotiations, or diplomatic image campaigns. Unlike economic or military warfare, the main instrument is politics and diplomacy, not material resources or physical force.

Cyber operations refer to the use of computer systems and digital technologies to attack, defend, or manipulate an adversary's infrastructure. The effects can be direct on data and infrastructure or indirect, through the impact on the target's

cognitive and psychological processes (Haataja, 2022, pp. 423-445). Examples include cyber attacks on critical infrastructure, ransomware, manipulation of electoral databases, or compromise of communications systems. Unlike other types of warfare, the action is predominantly technological and digital.

Within the theory and practice of modern conflict, we can say that cognitive warfare is an emerging operational domain focused on influencing mental processes. Unlike traditional forms of warfare, which seek to have a direct impact on the physical strength or infrastructure of the adversary, cognitive warfare focuses on the perceptions, assessments, and decisions of actors, targeting how they interpret reality and react in an operational context. Conceptually, it differs from information, psychological, or cyber warfare in that it is not limited to manipulating messages or disrupting digital infrastructures, but seeks to reshape fundamental cognitive processes at the individual and collective levels.

CHARACTERISTICS OF THE COGNITIVE DOMAIN

The cognitive domain is distinguished by a series of defining features that make it a unique operational space that is difficult to control using traditional methods. Firstly, it is intangible, as its actions do not produce direct and visible effects on the physical environment, but rather operate on the minds and internal thought processes of individuals or groups. This intangibility makes it difficult to measure success or assess the tactical or strategic impact of interventions.

Second, the cognitive domain is both individual and collective. At the individual level, cognitive warfare targets the processes of perception, attention, memory, and decision-making, seeking to alter how information is interpreted and integrated. At the collective level, the impact extends to public opinion, social cohesion, and cultural norms, influencing group behaviours and their ability to respond coherently. This duality requires approaches that combine psychological, sociological, and cybernetic analysis, integrating interdisciplinary perspectives for a comprehensive understanding of the cognitive domain.

Thirdly, the cognitive domain is based on perception (Claverie, du Cluze, 2023, pp. 1-13), which implies that operational reality is constructed subjectively. Unlike physical or digital environments, where the effects of actions can be measured objectively, in the cognitive domain, success depends on how information and messages are perceived and interpreted. Thus, manipulating information flows, introducing subtle misinformation, or amplifying emotions and prejudices become central tools in cognitive warfare, as they directly influence the target's decision-making and risk-assessment processes.

COGNITIVE WARFARE AS THE SIXTH OPERATIONAL DOMAIN

Recognizing the cognitive dimension as the “*sixth operational domain*” (Le Guyader, Cole, 2022, pp. 1-5) of contemporary conflict is an essential conceptual step in integrating this perspective into modern military doctrine. In the classical tradition, military operations are conducted in the land, sea, air, space, and, more recently, cyber domains. The introduction of the cognitive domain reflects the recognition that strategic success no longer depends exclusively on physical or technological superiority, but also on the ability to influence the adversary’s decision-making processes and perceptions.

This concept has been reinforced in the literature by identifying the interdependencies between the physical and cognitive domains: military conflicts on land, in the air, or in cyberspace can have limited effects if they are not accompanied by strategic management of the adversary’s perceptions and decisions. In this context, cognitive warfare becomes an emerging operational domain that not only complements but redefines the dynamics of modern conflict, highlighting the importance of integrating cognitive components into the planning and execution of military and non-military operations.

With regard to the role of artificial intelligence, social networks, and big data (<https://www.oracle.com/ro/big-data/what-is-big-data/>), recent technological developments have amplified the importance of the cognitive domain, making it a critical operational one. Artificial intelligence (AI) plays a central role in the rapid processing of massive amounts of data and in modelling target behaviours (Deppe, Schaal, 2024 pp. 1-6). Machine learning algorithms enable the identification of patterns of thought and behaviour in individuals or groups, facilitating the design of more precise and adaptive influence campaigns. In addition, AI can be used to generate content, simulate response scenarios, or optimize cognitive strategies, increasing the effectiveness of actions on the perceptions and decisions of the adversary.

Social networks are the central infrastructure through which a significant part of cognitive warfare is conducted. They allow for the rapid and targeted dissemination of messages, the amplification of emotions, and the polarization of opinions. Unlike traditional media, social networks offer the possibility of instant feedback and allow for the adaptation of influence campaigns in real time, transforming communication into a dynamic and interactive process.

Big data complements this architecture, providing unprecedented analytical resources for understanding collective behaviours and cognitive susceptibilities. Quantitative analysis of big data allows for the identification of population

segments vulnerable to certain messages, the evaluation of campaign impact, and the adjustment of strategies to maximize the effect on cognitive processes. The integration of AI, social networks, and big data thus transforms cognitive warfare into an operational domain characterized by speed, complexity, and adaptability.

SPECIFIC TACTICS OF COGNITIVE WARFARE

Cognitive warfare manifests itself through a wide range of indirect actions, unscrupulously targeting the human mind and social cohesion, including multiple forms of psychological pressure, information manipulation, and institutional undermining, which take the form of the following types of actions:

Actions aimed at undermining the morale of the civilian population – this type of actions targets social, professional, demographic, and geographic categories, adapting its messages and vectors to exploit the specific vulnerabilities of each group (from the elderly and single parents to workers in affected industries, students, ethnic or religious minorities, social protection, access to services, or discrimination, and geographically, campaigns exploit perceptions of rural marginalisation or urban pressures – housing, transport, health) (Munteanu, pp. 10-18).

Actions that diminish citizens' standard of living – against the backdrop of public discontent, cognitive warfare amplifies its effectiveness by using misinformation and emotional manipulation to exploit social frustrations and accentuate perceptions of economic and political injustice. *"The decline in living standards is exacerbated by information campaigns that induce panic, stimulate the division of personal or collective opinions, and undermine the legitimacy of public decision-makers, deliberately seeking to dramatically lower citizens' living standards by creating economic, financial, social, and health crises"* (UNDP, pp. 85–102). In this climate of tension, citizens become more prone to irrational collective decisions (panic buying, capital withdrawals, spontaneous protests), which generates economic instability and additional pressure on the political system, forcing the redirection of public resources from development to the management of informational and social crises.

Intergroup antagonism between different social categories – mechanisms that generate and amplify conflict act on the community by cultivating the perception that certain social categories are undeservedly privileged and have resources or rights that, in fact, do not belong to them. This strategy aims to create division between segments of the population, inducing a sense of injustice and fuelling tensions based on perceived inequalities. Manipulative information campaigns reinforce the image of certain privileged groups to the detriment of others, a process that promotes social division, undermines collective solidarity, and erodes social cohesion.

Actions that weaken national economic capacity – that manifest themselves through subtle mechanisms that influence strategic decisions, causing decision-makers to adopt policies and measures that weaken the industrial base. Under the impact of information campaigns and persuasive narratives, decision-makers are persuaded to close, sell, resize, or outsource industrial production, citing pretexts such as excessive pollution, lack of profitability, lack of raw materials, avoidance of trade union movements, insufficient funds for re-engineering, the absence of markets, or even the encouragement of foreign investment (Galeotti, pp. 85-112). Discourses that minimize the importance of strategic resources for the national economy or the need for major infrastructure (such as highways) are also promoted, thus justifying the processes of deindustrialization. The result of these actions is the closure of factories/companies, the reduction of domestic production capacity, and increased external economic dependence, which significantly weakens national security and lowers the standard of living of the population.

Actions to coerce and influence a state outside of military occupation – the aim is to induce policies and decisions that gradually (using the technique of small steps) lead to the loss of economic and financial-banking sovereignty, the surrender of control over critical infrastructure, national resources, capital flows, and even the workforce. Through persuasive discourse and informational pressure, decision-makers are steered towards measures that favour the alienation of public and private property, tipping the balance of agricultural land and strategic resource ownership in favour of external entities. At the same time, risk insurance systems and social protection mechanisms are compromised, reducing the state's ability to protect its citizens and domestic economy (Galeotti, pp. 113–139). Overall, these actions aim to gradually integrate the target state into a framework of structural dependence, whereby economic, financial, and social decision-making is diverted from the national interest to the interests of external actors.

Actions that undermine the functionality of critical systems – through manipulative discourse and policies promoted under the pretext of reform (Ib., pp. 8–20), actually aimed at dismantling the functional systems of society, eliminating vital elements without proposing viable replacement solutions. These actions directly or indirectly target essential segments of social and state infrastructure – education, the pension system, social assistance, justice and the legislative framework, the health system, as well as the financial, economic and commercial architecture, environmental protection and research capacity – eroding institutional cohesion and the capacity to provide public goods. Consequently, what is presented as modernisation, if not kept under legal control, becomes in practice a process of structural weakening that amplifies social vulnerabilities and reduces national resilience.

Military operational actions – the primary objective of this type of actions is not necessarily the physical destruction of the adversary's combat capability, but rather the induction and maintenance of a perceived state of imminent threat (Giles, 2022, pp. 8–20) – a persistent psychological pressure capable of degrading decision-making, internal cohesion, and the political will to respond effectively.

From a theoretical perspective, this dimension combines elements from studies on hard/soft power and from strategic game theory based on uncertainty: the aim is to maximize the perceived cost of a reaction from the target, without necessarily crossing the threshold of open confrontation. The operational mechanism is based on the synergy between material manifestations (military capabilities, shows of force) and non-material manifestations (narratives, information manipulation, subversive foreign policy), so that the threat remains credible and persistent.

The tactics used to achieve this cognitive pressure include, without providing operational instructions, the development and display of superior military capabilities (which fuel the perception of technical and military superiority), the conduct of shows of force and exercises with a deterrent role in the vicinity of borders, limited penetrations or incursions that test reaction thresholds, as well as political and administrative initiatives (e.g., the creation of autonomous enclaves governed by ethnic minorities) designed to erode the sovereignty and internal cohesion of the targeted state. The deliberate activation of frozen conflicts (Bargués et al., pp. 8-20), the justification of interventions through the rhetoric of minority protection, airspace and maritime violations, or illegal practices regarding the treatment of prisoners are all tools that amplify the feeling of vulnerability and uncertainty.

The intended effects are multiple and interconnected: disruption of the command-and-control process, intensification of information jamming (contradictory information, deliberate noise), erosion of domestic public and political support for security policies, weakening of internal and external ties (alliances), and induction of strategic or tactical errors on the part of the adversary. The strategy relies on the fact that decisions made under pressure are more susceptible to cognitive errors (excessive optimism, distortion of normality, overreactions, passivity).

From a legal and ethical perspective, these practices raise significant issues: many of the actions mentioned may violate international law (territorial sphere, protection of civilians, treatment of prisoners) and ethical standards of political-military leadership. In addition, the use of information manipulation and synthetic deepfake technologies (Barela, 2024/2025, p. 1) amplifies the risk of eroding public trust and fragmenting the information space, affecting the long-term resilience of societies.

Actions aimed at undermining military cohesion and morale – this type of actions deliberately targets the destruction of trust: in military and political-military leadership, in the legitimacy of the cause for which they are fighting, and in the reliability of the weapons and logistics on which the military entity relies. By eroding this trust, not necessarily through physical force, but through informational and symbolic campaigns that cast doubt on the competence, honesty, and purpose of the leadership or the safety of the equipment, the aim is to transform the motivation and individual and collective behaviour of the military.

The expected effect is progressive and holistic: initially, demotivation and a decline in confidence appear, which can evolve into segments of personnel abandoning the fight, then into a total loss of will to fight, and finally into a replacement of military order with indiscipline, disorganization, chaos, and insubordination. This decline creates a vicious circle: the loss of discipline facilitates the spread of rumours and panic, which in turn increases the receptivity of military personnel to new cognitive attacks.

The psychosocial mechanisms involved are based on compromising trust capital (legitimacy, competence, integrity), exploiting cognitive errors (confirmation, availability), and attacking social cohesion (exacerbating ethnic, professional, or economic tensions). From an informational perspective, the strategy combines credibility reduction (coupled with amplification of informational “noise”) with symbolic actions designed to discredit leaders and undermine cohesion and morale in military units.

The operational consequences are severe: degradation of command-and-control capabilities, erosion of coherent response capabilities, increased error rates and decisions made under pressure, as well as an increased risk of institutional collapse in the affected structures. In strategic terms, the objective is not necessarily immediate physical destruction, but rather neutralizing the adversary’s ability to leverage its human and moral resources.

Political compromise actions – this type of actions targets a whole set of informational practices designed to distort collective representations, degrade decision-making capacity, and reconfigure the political power structure by exploiting cognitive and algorithmic mechanisms.

In this logic, political compromise operations (blackmail, intentional disclosures of information, deepfakes, discredit campaigns) are mobilized to draw high-ranking political elites to one side, to generalize and exaggerate reprehensible acts, and thus to discredit individuals regardless of their achievements, a phenomenon that undermines the credibility of actors and institutions.

At the same time, narrative manipulation and polarizing amplification (through social platforms, networks of automated accounts, and complicit media) sow irreconcilable contradictions between factions, fuel internal controversies, and stimulate ideological hatred, resulting in prolonged political crises and social fragility.

At the strategic level, external actors/parties have used institutional capture mechanisms to ensure the loyalty of the administrative leadership – frequent promotion/rotation of politicians in key positions, replacing technical experts with political figures, supporting doctrine and legislation favourable to the economic interests of certain groups and, in extreme cases, facilitating the emergence of politically affiliated paramilitary groups, all in order to undermine the continuity of state projects, encourage corruption, and maximize political division.

Therefore, based on the examples listed, we can provide a convincing picture of the socio-political contexts in which cognitive warfare becomes operational as well as of its destructive effects. The combination of different tactics, in varying proportions, aims to maximize impact, and the cost-effectiveness ratio of these operations is significantly more favourable to the aggressor than that of conventional military means.

CONCLUSIONS

Cognitive warfare is an emerging operational domain aimed at shaping the mental processes, perceptions, and decisions of both individuals and communities. Unlike traditional conflicts, which focus on immediate kinetic effects, this form of conflict frequently resorts to non-kinetic instruments – propaganda, disinformation, psychological operations, and digital means – designed to restructure the way information is processed and interpreted, thus generating lasting strategic effects.

The integration of digital technologies, social platforms, big data analytics, and artificial intelligence significantly amplifies the effectiveness of cognitive operations, increasing the speed of response, adaptability, and micro-targeting capabilities of influence campaigns. Consequently, the cognitive dimension is becoming a central factor in contemporary geopolitical strategies, with repercussions on social cohesion, institutional resilience, and the level of trust between state actors.

Institutional and normative divergences between political regimes outline a paradox of cognitive vulnerability: democracies, through transparency and informational pluralism, are increasingly exposed to manipulation and division, while authoritarian regimes show structural resilience to such attacks, often achieved by restricting civil liberties. At the same time, cognitive warfare intersects with strategic persuasion tools and psychological operations, integrating normative,

emotional, and cognitive influence into a coherent strategic framework on an international scale.

The impact on collective security and international law is considerable: the erosion of trust between states, the fragmentation of coalitions, and regulatory gaps regarding non-kinetic aggression raise complex issues of regulation and response. The political response requires the development of vectors of societal resilience, international standards of transparency, and coordinated mechanisms for counteraction and harmonization.

In this context, conceptualizing cognitive warfare as a “*sixth operational domain*” emphasizes the need to integrate the cognitive dimension into strategic planning and international security architecture, recognizing the influence on perceptions and decisions as a central element of current strategic dynamics.

BIBLIOGRAPHY:

1. Babacek, M. (2024). *Războiul cognitiv: Opriți competiția mondială pentru “Controlul creierului uman”*, in Revista Art – Emis Academy.
2. Barela, S.J. (2024/2025). *Digital Disinformation Operations in Armed Conflict* – Info-Brief. Switzerland: Geneva Academy of International Humanitarian Law and Human Rights.
3. Bargués P., Bourekba, M., Colomina, C. (2022). *Hybrid threats, vulnerable order*, CIDOB Report.
4. Cîrstocea, I. (2016). *Religia ca factor de conflict și război*, in *Impact Strategic*, no. 1. București: Editura Universității Naționale de Apărare “Carol I”.
5. Claverie, B. du Cluzel, F. (2023). *Cognitive Warfare Concept*. Innovation Hub – Allied Command Transformation (ACT), NATO.
6. Deepe, C., Schall, G.S. (2024). *Cognitive Warfare: A Conceptual Analysis of the NATO ACT Cognitive Warfare Exploratory Concept*, *Frontiers in Big Data*, vol. 7.
7. Galeotti, M. (2022). *The Weaponisation of Everything*. A Field Guide to the New Way of War. Yale University Press, New Haven.
8. Giles, K. (2016). *Russia’s ‘New’ Tools for Confronting the West*. Chatham House Research Paper.
9. Haataja, S. (2022) *Cyber operations against critical infrastructure under norms of state behaviour in cyberspace*, in *International Journal of Law and Information Technology*, vol. 30, no. 4.
10. Hoffman, F.G. (2007). *Conflict in the 21st Century*. The Rise of Hybrid Wars.
11. Joint Publication JP 3-13: Information Operations (updated 2014).
12. Miller, G.A. (1956). *The Magical Number Seven, Plus or Minus Two: Some Limits on Our Capacity for Processing Information*, in *Psychological Review*, Washington, D.C., vol. 63, no. 2.
13. Mouslim, H. (2025). *Coercive Diplomacy Recalibrated: Evaluating Effectiveness, Risks, and Modern Challenges*, in *African Scientific Journal*, vol. 3, no. 29.

14. Munteanu, D. (2022). *Barometrul rezilienței societale la dezinformare*. Euro-Atlantic Resilience Centre (E-ARC).
15. Naganuma K. (2021). *Warfare in the Cognitive Domain: Narrative, Emotionality, and Temporality*, NIDS Commentary no. 163, National Institute for Defense Studies Japan.
16. Neacșu, I. (2004), *Războiul psihologic. Tehnici și strategii de influență*. București: Editura Militară.
17. Neisser, U. (1967). *Cognitive Psychology*. Prentice Hall.
18. Popa, I. (2018). *Războiul economic: forme, mijloace și efecte*, in *Revista de Științe Militare*, no. 2. București: Editura Centrului Tehnic-Editorial al Armatei.
19. Thomas, T.L. (2025). *Russian Military Thought: Concepts and Elements*, TRADOC G-2/OE Watch.
20. UNDP (2022). *Human Development Report 2022*. Uncertain Times, Unsettled Lives, UNDP, New York.
21. Voicu, M. (2018). *Matrioșka mincinoșilor: fake news, manipulare, populism*. Editura Humanitas.
22. Zodian, V. (2019). *Impactul progresului tehnologic asupra conflictelor armate contemporane*, in *Impact Strategic*, no. 3. București: Editura Universității Naționale de Apărare “Carol I”.
23. <https://brainly.ro/tema/6593720>, retrieved on 11 September 2025.
24. <https://www.oracle.com/ro/big-data/what-is-big-data/>, retrieved on 15 September 2025.

THE ROLE OF THE BODY IN COGNITION – APPLICATION IN SPORTS AND MILITARY INSTRUCTION –

Military Student Daria Ștefania MIHALCEA

*Faculty of Physical Education and Sport-Technical Military Academy of Bucharest,
Faculty of Psychology and Education Sciences, Cognitive Sciences*

DOI: 10.55535/RMT.2025.3.11

This essay proposes the idea that an individual's body has an undeniable role in the understanding of the concrete world. Embodied cognition is an approach to cognition that puts emphasis on locomotion, which is one of the most important ways an organism receives sensory signals about the environment. 4E Cognition theory has as a core idea the fact that our mind is not limited only to the brain, and it expands throughout the whole body and also in the environment. This view came as an opposition to Descartes' ideology that supports the existence of the mind without a body. Furthermore, 4E Cognition critiques traditional cognitive psychology, which is strongly influenced by computationalism, which classifies the mind as an abstract information processor and places minimal importance on the mind's connection to the outside world.

This paper argues that the body is an essential tool that provides information about the exterior world and influences cognition. This idea connects to the way an athlete or a soldier perceives and manages information through the body's motion, therefore the study explores how bodily experience shapes perception and action by making use of the comprehensive framework provided by the embodied cognition theory, giving representative examples from sport and military contexts.

Keywords: embodied cognition; perception; physical performance; military instruction; automatisms;

INTRODUCTION

The mind as a complex internal structure offers multiple perspectives regarding cognition and how it works. I advocate the view that the body's role in cognitive processes is essential, and that embodied cognition explains the best how it is possible. In this regard, athletes and soldiers provides the best examples that demonstrate exactly how repeated movements and physical actions improve certain cognitive processes and influence perception and mental activity. This idea contradicts the view that physical performance is based solely on muscle memory or automatisms, and that it does not have any effect on the mind and does not influence our way of thinking.

4E Cognition theory best presents the importance of our bodies in our understanding of the world and the way our interaction with the environment directly shapes how we perceive reality. By supporting this view, there seem to be important consequences for professional athletes and soldiers considering the number of physical trainings they do and how they constantly work with specific objects that also influence their cognition and how they relate to the environment.

4E COGNITION IN SPORTS AND MILITARY INSTRUCTION

The approach proposes that cognition is not limited to our heads, that it is embodied, enacted, extended and embedded. It contradicts the traditional views which argue that cognition occurs in the head through mental representations of states of affair, which are interpreted symbolically and generate an action, a response.

Sports and military domains generate valuable input that successfully defends the 4E cognition theory. There are several examples that can be taken into consideration. In sports such as tennis, canoeing, baseball, athletes must make use of certain objects from the environment, such as rackets, paddles, bats, in order to perform tasks required by that specific sport. These objects help them understand how the movement works, the biomechanics behind it, and ultimately, they represent ways in which players and soldiers understand the properties of the environment by their interaction within it.

In military instructions, soldiers work with weapons and perform specific physical activities that require always having such objects at hand and learning

to control movement and actions while handling these tools. A consequence would be that soldiers get used to the physical properties of the object, and they redefine their motions in correspondence with it and the way it works. It has an important effect on their mental representation of the environment, which subsequently provides necessary structure and support for them to effectively think and act. These ideas show how embedded cognition applies to sports and the military domains and they also highlight the importance of embedded cognition in skill acquisition, a central part of sports and military physical practice.

In terms of extended cognition, the objects mentioned previously and defined as external tools become extensions of the mind because they serve a purpose that is completed by manipulating them in the intended way. For instance, in tennis, the interaction of the agent with the racket causes the ball's change of trajectory. In this way, the immediate state of affairs modifies according to the knowledge that the player has about the tool used and its properties, therefore the racket constitutes a part of the agent's cognitive function.

The same rationale applies to the soldier in his interaction with weapons and equipment within contexts of tactical operations. Soldiers integrate weapons to their body schemas, by repeatedly interacting with them. Therefore, they extend their sensorimotor system and act in accordance to a renewed mental configuration of their own persona. It happens as an effect of the "*extended mind*", which adapts mental processes in order to improve cognition by relying on the body's activity in the environment.

Another view to extended cognition associates the knowledge and intentions of a larger group of people that serve a common purpose, the case of military groups being relevant in this respect. In this case, the coupling between systems is mediated by language (Clark, Chalmers, 1998). This socially extended cognition could be represented successfully by how a sports team functions during a match or a performance and how a platoon manages to cooperate and apply certain field strategies. There seems to be an exterior conscience of the group, which "*acts*" and "*thinks*" according to the guidelines imposed by game regulations, specific tactics and trained movements.

Practicing sports at a performance level implies repetition of specific movements and repeated usage of certain aptitudes, and an effect is that athletes develop a different perception of the world. For example, behaviour is influenced by sport activities, which in the long term impose certain values that athletes have to acquire and integrate in their own value system. Consequently, using this concept, it could be easily argued that *"the perceived world is a consequence of the actions the body*

takes toward it” (Cappuccio, 2019). In this case, sports model an agent’s world by requiring both physical activity and certain mental processes that influence the overall perception.

This is also the case in the military domain, because soldiers take repeated actions and exercise certain tactics and movements that restructure their perceptual map and creates automatisms and certain “*neural shortcuts*” that ultimately constitute the basis of performance in the military field action.

These ideas lead to the same conclusion, that enacted cognition plays a central role in the athlete’s physical and mental development, and it also justifies the superior cognitive abilities that athletes and soldiers exert during their physical performances.

COGNITION IN AUTOMATISMS

Skill acquisition in sports and military instruction is considered a process from an initial cognitive phase to a superior phase where performance becomes automatic. This view includes the action of muscle memory, which allows an athlete and a soldier to pay less attention to their movements, because they require less conscious action. In this way, they manage to focus more on variables that interfere with their performances, exterior stimuli such as the opponent’s actions, the public or commanders, weather and other potential stressors.

Motor skills development consists of three stages of learning (Fitts, Posner, 1967). These three stages are represented by *the cognitive stage*, *the associative stage* and *the autonomous stage*. The focus is going to be on the last stage, because it is the most common process among professional athletes and soldiers and the way it works offers important insights into their cognitive abilities.

Automaticity is an advanced cognitive process that is accessed through repetition and constant training. As opposed to perspectives that argue against the role of cognition in advanced physical skills, the main idea is that, in complex automatized movements, cognition plays a central part.

It is generally believed by coaches, superiors and even athletes and soldiers that the actions they perform after long periods of training, in competitions and in battles, is only limited to their bodies. Moreover, it is also considered that it is an almost immediate reaction of the body in certain contexts, such as field tactical exercises with troops or sport championships, which does not require anything from the mind, being just the body’s reaction to intensive trainings. The whole concept of embodied cognition is in opposition to approaches such as this, because the perspective of embodied cognition presents a unitary cognitive

system compounded of the body and the mind, which functions as a whole. Therefore, this holistic approach of cognition excludes the possibility of physical performance without the cognitive counterpart.

In order to create a better understanding of the automatisms displayed in elite athletes and soldiers, this paper clarifies certain aspects that influence their extremely precise and efficient movements. Athletes and soldiers have superior cognitive skills at the level of perception, anticipation and decision-making. Their trained skills include an advanced reaction time with great coordination between the interpretation of exterior stimuli and their mental and physical response. These aspects, presented in the light of the mirror neurons action, reveal the common neuronal basis of action observation and execution. It is also empirically demonstrated that when athletes and soldiers develop their skills in certain moves, their perception regarding contexts that include those moves will enhance considerably (Schorer et al., 2018). Given the perspective that perception is a *“trainable”* mental process among others, there are two important consequences that deserve to be mentioned:

- Firstly, physical exercises performed repeatedly lead to a special mental development experienced by elite athletes and soldiers. In this way, certain cognitive components are enhanced. The architecture of the mind seems to remodel, to adapt to the actions performed by the body. Therefore, the analysis suggests that intensive physical trainings that test the limits of the body help both athletes and soldiers to have a better understanding of their physical capacities and to develop mental abilities that support and facilitate their actions by transferring part of the cognitive load, prominent in cognitive and associative stages, to the body, therefore resulting in the autonomous stage. It does not undermine the action of the mind, but simply shows how it is distributed across the body and the environment with the purpose of enabling the athletes and soldiers better concentrate on things that they cannot control instead of directing energy and attention towards actions that could be internalized and ultimately automatized.

- Secondly, this *“shift”* illustrates the flexibility of the mind and how it can adapt to stressful and intense situations. Thus, when a movement or physical procedure is internalized, the body manages to *“take control”*, especially when the mind is preoccupied with other aspects. Here is important to note the distinction between conscious action and cognitive action. Automatic moves occur more often than not unconsciously when the agent has his attention distributed towards external or even internal factors that could disrupt his performance. In this way, the body's automatic response could be seen as an *“autopilot”* that takes control whenever

other situations that need to be taken care of emerge. That is why, in trainings, athletes and soldiers must be fully conscious and focused on the movements they perform, in order to assimilate and comprehend how they are executed. Only after fully understanding the biomechanics behind it, can athletes and soldiers start the repetition process required by the automatization of the process. This aspect provides evidence that the action of the body is crucial in cognition and has an important role in the way we process information and react to it.

IMPORTANCE OF THE TOPIC

Combating existent stereotypes in the sport and war collective is extremely important because coaches and commanders that do not understand the power of the mind in sports and battles fail to help their students complete a holistic preparation.

Being aware of the powerful connection between body and mind would help specialists in sports and military instruction focus on developing balanced programs, to train more efficiently the mind along with the body. Techniques that focus more on the contribution of mental processes in the action of the body would optimize the movements performed and provide insights about the body-mind connection that could contribute to the soldiers' and athletes' self-image and overall physical and mental performance.

In the sports domain, integrating specialized trainings that put emphasis on strengthening the connection between body and mind would help athletes develop at a superior level by forming a better understanding of their own bodies and the environment they act upon (Aman et al., 2015).

In the military field, soldiers' mental representations and body-control play a vital role in their activity. The stressful environment and demanding conditions require both mental and physical strength and stability. In addition, soldiers must remain focused and highly vigilant at all times during their operations, they must take fast decisions and overall process data at a very high level. Therefore, the relationship they establish with the environment is essential because they constantly interact with external objects and persons and subsequently develop a mental schema that is in accordance with their immediate reality. Embodied cognition mediates this process by providing the necessary tools for developing a global knowledge that connects data from the environment with mental activity.

Explaining aspects of cognitive sciences by using examples from sports and military fields and vice versa represents a way in which these three domains can gain valuable input and new perspectives can be explored. It is also the evolutionary perspective that provides important ideas regarding the evolution

of physical exercises and of cognition. For instance, natural selection, the process that favours individuals with certain physical abilities which would survive in dangerous situations, could be interpreted as a trigger to more complex cognitive functions. In this sense, the body's actions in an environment would conduct to a better understanding of the world and a manifold perception that is related to complex mental processes.

CONCLUSIONS

In kinesiology, physical exercises are defined as tools that allow athletes incorporate in a rational way an informational content. This definition clarifies that cognition is strongly influenced by the actions of the body in the environment, view sustained by embodied cognition as well as extended cognition, embedded cognition and enacted cognition. These all put value on the physical interactions and the way an individual perceives the exterior world based on his direct experience.

The 4E (embodied, enacted, extended, and embedded) framework for cognition offers a solid alternative to more traditional views that limit cognition to internal mental representations. Evidence from sports and military contexts illustrates how interactions with tools, objects, and group dynamics extend and shape cognitive processes, restructure perception, and enhance skill acquisition. Through repeated practice and physical activity, athletes and soldiers integrate objects and actions into their cognitive systems, demonstrating that thinking and understanding are deeply intertwined with bodily activity and environmental interactions. In other words, mental processes are directly shaped by physical activity and experience with external objects. These domains provide strong support for the relevance and applicability of 4E cognition in real-world, performance-driven contexts.

The “*activation*” of automatisms requires using specialized and superior mental functions that act rapidly, without the agent being fully conscious. It does not result in actions without “*the mind's presence*,” but more likely in actions with the presence of complex and trained cognitive processes.

All the ideas presented in this essay support the same perspective, that the mind is present in all physical interactions and that the physical activity in the environment manages to develop cognition significantly.

BIBLIOGRAPHICAL REFERENCES:

1. Aman, J.E., Elangovan, N., Yeh, I.-L., Konczak, J. (2015). *The effectiveness of proprioceptive training for improving motor function: A systematic review*, in *Frontiers in Human Neuroscience*, 9, Article 655, <https://doi.org/10.3389/fnhum.2015.00655>, retrieved on 10 September 2025.

2. "Brain Games: Inside the Brain of the Elite Athlete", in *Queensland Brain Institute – University of Queensland*, 19 January 2017, qbi.uq.edu.au/blog/2016/09/brain-games-inside-brain-elite-athlete, retrieved on 8 September 2025.
3. Carney, J. (2020). "Thinking Avant La Lettre: A Review of 4e Cognition". *Evolutionary Studies in Imaginative Culture*, U.S. National Library of Medicine, 2020, [pmc.ncbi.nlm.nih.gov/articles/PMC7250653/](https://pubmed.ncbi.nlm.nih.gov/articles/PMC7250653/), retrieved on 20 August 2025.
4. Clark, A., Chalmers, D.J. (1998). *The extended mind. Analysis*, 58(1), pp. 7-19, <https://doi.org/10.1093/analys/58.1.7>, retrieved on 22 August 2025
5. Descartes, R. (1641/1996). *Meditations on First Philosophy*. Cambridge University Press.
6. Haggard, P. (1970). "Patrick Haggard, Conscious Intention and Motor Cognition", in *Phil Papers*, 1 January 1970, philpapers.org/rec/HAGCIA-3, retrieved on 20 August 2025.
7. *Handbook of Embodied Cognition and Sport Psychology* (MIT Press): Cappuccio, M.L.: 9780262038508: Amazon.Com: Books, www.amazon.com/Handbook-Embodied-Cognition-Sport-Psychology/dp/0262038501, retrieved on 5 September 2025.
8. Schorer, J. et al. (2018). *Modified perceptual training in sport: A new classification framework*, in *Journal of Science and Medicine in Sport*, 21(9), pp. 950-958, <https://doi.org/10.1016/j.jsams.2018.01.011>, retrieved on 5 September 2025.
9. Shapiro, L., Spaulding, S. (2025). *Embodied Cognition*, in *The Stanford Encyclopedia of Philosophy* (Summer 2025 Edition), Zalta, E.N., Nodelman, U. (eds.), <https://plato.stanford.edu/archives/sum2025/entries/embodied-cognition/>, retrieved on 20 August 2025.
10. Wulf, G., Prinz, W. (2001). *Directing Attention to Movement Effects Enhances Learning a Review*, in *Psychonomic Bulletin & Review*, 8, pp. 648-660. References - Scientific Research Publishing, <http://dx.doi.org/10.3758/BF03196201>, retrieved on 10 September 2025.
11. "'4E' (Embodied, Embedded, Enactive, Extended...) Cognition". *Cognitive Classics*, 19 May 2017, cognitiveclassics.blogs.sas.ac.uk/hums-list/4e-embodied-embedded-enactive-extended-cognition/, retrieved on 20 August 2025.

THE NEW LIGHT CAVALRY OF THE 21ST CENTURY – ANALYSIS OF THE INNOVATION AND EMPLOYMENT OF MOTORCYCLE ASSAULT GROUPS BY THE RUSSIAN ARMY IN THE UKRAINE WAR –

Colonel Marius GHEORGHESCU

The 307th Naval Infantry Regiment “HERACLEEA”

DOI: 10.55535/RMT.2025.3.12

Given the increasing speculation regarding the effectiveness of Motorcycle Assault Groups, especially on a relatively static battlefield oversaturated with artillery, missile and drone operations, we have conducted a focused investigation to better understand this evolving tactic. This article provides a first-hand assessment of the organization, tactics, and equipment of the Motorcycle Assault Groups of the Russian Armed Forces as of June 2025. The article is based primarily on open-source information, published documents captured at the tactical level by the Armed Forces of Ukraine, reports from Ukrainian infantry fighting in contact, images/video captures from Ukrainian frontline surveillance drones, publicly available interviews with motorcycle crews of the Russian Armed Forces, and even available official reports issued by the Armed Forces of Ukraine.

Keywords: motorcycle assault groups; FPV drones; assault tactics; reconnaissance-surveillance; portable C-UAS system;

INTRODUCTION

The short time between detection and engagement, driven by real-time surveillance with reconnaissance drones and the high response speed of FPV attack drones, has created a particularly hostile environment for the use of traditional armoured tactical vehicles (tanks, infantry fighting vehicles/IFVs, armoured personnel carrier/APCs) on the modern battlefield. As a result, both forces involved in the Ukraine War have been forced to adapt rapidly and in a highly innovative manner.

Such adaptation first appeared in 2024, when the first *motorcycle assault groups* of the Russian Armed Forces began to be seen with increasing frequency along the Russian-Ukrainian frontline. Their presence quickly attracted public attention, and their use in combat has since become a common feature of front-line combat engagements. More recently, Ukrainian forces have also announced the establishment and training of their own motorcycle assault units (Bussines Insider, 2025).

Throughout recent history, motorcycles have been a feature of unconventional/ guerrilla warfare, particularly among non-state actors in regions such as Africa. However, their use by modern professional state armies has traditionally been limited to reconnaissance roles through patrols or, at most, light logistic support. This has changed dramatically in the Russo-Ukrainian war, where the widespread use of unmanned aerial systems/UAS, particularly FPV drones, has reshaped battlefield tactics. A recent study by RUSI (Royal United Services Institute) estimated that drones were responsible for 60-70% of the damage or destruction of Russian military systems. In this environment, traditional armoured vehicles – once essential for manoeuvre warfare – have become extremely vulnerable. This has led both Russian and Ukrainian forces to adapt, increasingly relying on motorcycles and ultra-light all-terrain vehicles (All-Terrain Vehicle/ATV, buggy¹) to increase mobility, speed and flexibility of infantry in particular. These vehicles are now used

¹ “Buggy” is a term generally used to refer to any light (ultra-light) automobile with off-road capabilities and minimal bodywork. Most are built either as vehicles assembled from parts of different origins or entirely from scratch. The word “buggy” was originally used in Great Britain to describe a light two-wheeled carriage for a single person and later in the United States to describe a common four-wheeled carriage. The term was extended to light automobiles as these became popular. The term briefly fell out of use before being revived to describe more specialised off-road vehicles (author’s note).

not only for assault, but also for reconnaissance, logistical support (resupply, medical evacuation, etc.) and support for tactical electronic warfare teams, especially in terrain where heavy armoured vehicles are ineffective or too easy to spot.



Photo 1: Motorcycle Assault Group from the 299th Parachute Regiment (VDV) of the 98th Airborne Division of the Russian Federation army, during a tactical field exercise (https://x.com/ukraine_world/status/1916823309989147027)

The war in Ukraine has evolved into a phase where any movement is determined by the massive presence of surveillance drones and artillery, missile or FPV drone strikes on the front line. More and more small (or ultra-light) vehicles are entering the action at the expense of traditional tactical armoured infantry vehicles (IFVs, APCs, tanks), which are slower and easier to detect. Following observations on the Pokrovsk front sector, three different Ukrainian infantry battalions provided some examples of the change in battlefield evacuation of the wounded: now this can only be done at night using ultra-light vehicles, such as buggy-vehicles. Ukrainian military analysts and those of its Western allies have noted the use of these vehicles in attacks by some units of the Russian Army since April 2024. Videos broadcast by Russian media and online military reports show a large fleet of all-terrain vehicles from regimental units of the 123rd Motorized Infantry Brigade in Donetsk (*photo 2*) or from the 71st Motorized Infantry Regiment on the Zaporozhye front.



Photo 2: Motorcycle Assault Group of the 123rd Motorized Infantry Brigade, presented on Russian television (El Pais, 2024)

In this latter case, images published by its staff show motorcycles on which metal cages have been installed to protect crew members from FPV drone attacks (*photo 3*).



Photo 3: Motorcycle belonging to the Russian army on which a protective cage against FPV drones was improvised (Telegraph, 2024)

In recent months, Russian soldiers have been recommending on their Telegram the use of electric motorcycles accounts because they are quiet and harder to detect by drones equipped with thermal imaging systems. *“Motorcycles are a good tactic because they are harder for drones to intercept, they are less noisy and faster than armoured vehicles or SUVs”*, says Andrii, a soldier with the 3rd Assault Brigade of the Ukrainian Armed Forces (El Pais, lb.), adding that *“the Russians are using them in large numbers and they are getting better”* (Telegraph, 2024). In another sector of the Donetsk front, in Kostiantinivka, a non-commissioned officer with the 93rd Mechanised Brigade of the Ukrainian Armed Forces confirmed the change in tactics to the newspaper *“El Pais”* on 8 June 2024: *“The Russians have everything for infantry transport, and now they have motorcycles. These are the worst, because they are difficult to detect, and our men cannot identify what that distant noise is”* (El Pais, lb.). The patterns of action of these Russian units that have been determined are the same with those of the soldiers of the 93rd Mechanised Brigade and the 3rd Assault Brigade of the Ukrainian Armed Forces: *“groups of eight soldiers from professional assault units ride four motorcycles, leaning at dusk or at night and, undetected, reach their front-line trench or directly attack Ukrainian positions”*. Rob Lee, a military expert at the US Foreign Policy Research Institute, confirmed last April on his “X” account that *“the advantage of the motorcycles is that they get to the trenches earlier and are harder to locate. The attacks are staged in coordination with artillery and FPV drones”* (lb.).

CONDITIONS FOR ADOPTION

One of the key conclusions of this research is that, before extrapolating the experience of the Russian Army Motorcycle Assault Groups to other theatres of operations or advocating for their adoption by other forces, we should first understand the subsequent challenges and battlefield conditions that led the Russian Army to pursue this adaptation in the first place.

In a battlefield where neither side holds air supremacy, and large-scale combined arms operations remain difficult to execute, combat has shifted to smaller tactical formations (small units) – typically at the squad, group, platoon, or at most company level, supported by armoured vehicles. In such a combat environment, traditional armoured platforms such as tanks, IFVs, or other types of armoured tactical vehicles face increasing challenges, especially in the context of constant artillery fire and the widespread use of cheap and fast FPV drones.

In response to these challenges and the accelerated depletion of reserves of armoured tactical vehicles, the Russian Armed Forces have increasingly relied on small tactical units that use covert movement and infiltration through uncovered spaces of the Ukrainian defence (or increasingly difficult to cover due to high personnel losses), to reduce the risk of detection. However, this comes at the cost of mobility and operational flexibility. Once detected, such groups are often quickly eliminated by FPV drone attacks or artillery fire. Even when they achieve tactical success, their ability to exploit gaps in Ukrainian defences is severely limited when operating on foot (dismounted). In these circumstances, the main factors that created the conditions for the emergence and increasingly widespread use of motorcycles on the battlefield are the following:

- a. *the persistent inability of the Russian Army to execute large-scale coordinated combined arms operations capable of breaking through Ukrainian defence;* even when Russian forces manage to form significant force groups (including hundreds of tanks, APCs, artillery systems, missile units, and air defence systems), they continue to struggle with the integration and synchronization necessary for effective combined arms offensive operations; as a result, Russian forces have switched to deploying small, inferior assault groups in small-scale but high-frequency attrition attacks; this approach focuses on *gradually exhausting* Ukrainian forces and identifying weaknesses that can be exploited later;
- b. *the lethality of well-prepared Ukrainian defensive positions, especially those supported by real-time reconnaissance-surveillance systems and high-precision strike systems;* on the modern battlefield, advanced surveillance systems allow defenders to quickly identify high-value targets, while precision massed fire makes it possible to neutralise attackers;
- c. *the limited number of personnel and their reduced ability to control/maintain the defence sectors held by Ukraine facilitate the passage (infiltration) of small mobile units of Russian forces through the defence;* unlike conventional light or armoured infantry groups, successful motorcycle infiltrations facilitate penetration deep into the rear area, while remaining more difficult to observe and block (neutralise) with artillery and, at the same time, more capable of neutralizing Ukrainian forces' FPV drones using portable electronic warfare (jamming) systems mounted on motorcycles;
- d. *high tolerance for personnel losses in offensive operations;* as will be discussed later in this article, the assault tactics of the Russian Motorcycle

- Assault Groups depend on the mass deployment of forces; the concept accepts higher losses among assault units, as long as a small portion of them manage to break through enemy lines and fulfil the mission objective;
- e. *lack of options for transporting troops with tactical armoured vehicles*; while Soviet-era infantry fighting vehicles (BMD family) or armoured personnel carriers (BTR family) are vulnerable to FPV drones, more modern Western-made armoured vehicles such as the Bradley or CV-90 offer better protection and have demonstrated better survivability for transported infantry during artillery strikes or FPV drones; the current fleet of tactical armoured vehicles of the Russian Army does not have a viable, mass-produced alternative to provide better protection for troops;
 - f. *Ukraine's geography and seasonal conditions favour mobility*; the dry and flat steppe terrain, with many forest/shrub patches and rural areas significantly increases the effectiveness of attacks using motorcycles; in contrast, heavy snow, mountainous areas or dense forests are much less suitable for this type of manoeuvre.

Once the advantages of Motorcycle Assault Groups became clear, we assessed whether their benefits could justify the risks. At around \$2,000-\$4,000/bike (depending on model and condition), these motorcycles are much cheaper and easier to replace than infantry fighting vehicles, with minimal maintenance costs. Their mobility and low profile allow them to traverse obstacles and evade detection more easily than larger platforms – especially when equipped with deployable electronic warfare systems on board. Concealed even in small buildings and nearly silent at night in the electric motorcycle variant, they maintain the element of surprise. A motorcycle can reach a position in minutes, outpacing a noisy and slower infantry fighting vehicle or tank and greatly reducing the response options of enemy FPV drones. Finally, motorcycles allow teams to carry heavier portable weapons – portable anti-tank systems/ATGMs, grenade launchers, or other support weapons – along the flanks, providing rapid and flexible fire support where it is needed most.

ORGANISATION OF FORCES

Despite the meaning of the term “*assault*” in their name (original in Russian – Штурмоваягруппамотоциклов/МШГр), these subunits are not used exclusively for direct assault. In practice, their roles are more diverse – from reconnaissance and diversionary manoeuvres to infiltration behind enemy defences, logistical support and support for enveloping manoeuvres during larger offensive operations.

More importantly, the motorcycle serves primarily as a means of rapid transport, transporting forces to assigned objectives rather than serving as a combat platform in its own right. According to some American military analysts, a relatively more accurate historical analogy can be seen with the “*dragoons*” troops, a type of light cavalry – infantry that moved on horseback to the combat zone, but dismounted to fight on foot. The Dragoons were used for reconnaissance, security, envelopment/flanking, and even close combat – tactical roles that closely resemble how the Russian Army’s Motorcycle Assault Groups are now used².

Russian motorcycle units have also begun to adapt. Reports from Ukrainian sources indicate that Russian assault motorcycles are equipped with iron cages to defend against drone attacks (*photo 2*) and in some cases, with portable electronic warfare (EW) equipment designed to jam approaching drones. These units are not just agile; they are increasingly networked and self-protected – illustrating a clear shift towards integrated and flexible force structures. The basic organisation of a Motorcycle Assault Group can vary depending on the unit, its assigned tasks, and the available resources of the unit to which it belongs. However, in general, such a group usually consists of 6 to 8 motorcycles, with 1 to 2 motorcyclists per vehicle, resulting in a total number of personnel ranging from 6 to 16 people on average (*figure 1*).

At least one motorcycle in the group is usually equipped with a portable drone scanner (mini-radar), which scans the area for the presence of FPV drones. In addition, these groups are expected to carry 2-3 portable C-UAS EW jamming systems, either mounted directly on the motorcycles or carried in a backpack by a biker, to disrupt communications between hostile (Ukrainian) drones and their operators during the assault (*photo 4*).

² “*Dragoons*” is a category of mounted troops that originally served as infantry using horses for transport, but fought on foot, although they later operated as conventional mounted cavalry. The name comes from a type of short musket or carbine – the “*dragoon*” (a pistol-like version of a trumpet that emitted a burst of fire when fired), carried by these soldiers. Dragoons were a versatile and cost-effective military force, serving in many European armies from the 17th century onward for tasks such as reconnaissance, security, raiding, and even acting as rearguard or support for infantry units. Dragoons were established in most European armies in the late 16th and 17th centuries, offering a cheaper option than traditional cavalry. Dragoons captured and held strategically important positions, such as bridges and passes. They also guarded camps and supplies, served as scouts, and performed police duties. As warfare evolved, dragoons increasingly served as conventional cavalry, often as medium or light cavalry. In the 20th century, dragoon regiments were often converted to armored units. The term has also been used for mechanized infantry units, reflecting their continued role in mechanised warfare. Today, some armored or ceremonial mounted regiments in various countries, such as the Royal Dragoon Guards of the British Army or the Royal Canadian Dragoons of Canada, retain the title “*dragoons*” (author’s note).

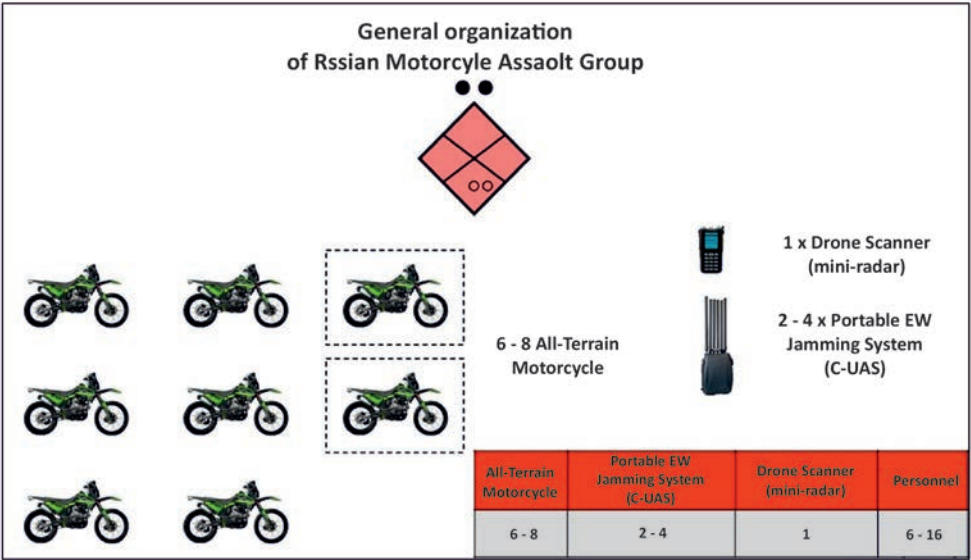


Figure 1: Organization and basic equipment of a Motorcycle Assault Group within Russian Army³



Photo 4: Soldier of the Russian Army equipped with a portable C-UAS EW system (Ib.)

Typically, motorcycles carry two passengers, with the passenger being the primary fighter, ready to engage both ground targets and aerial threats such as drones while on the move (photo 5). In some cases, motorcycles are equipped with a handlebar-mounted machine gun mount for the rider, allowing for limited firepower. However, a handlebar-mounted machine gun for the rider still appears to be quite uncommon in practice.

³ Adapted from [https://substackcdn.com/image/fetch/\\$s_!C6Eg!,f_auto,q_auto:good,fl_progressive:steep/https%3A%2F%2Fsubstack-post-media.s3.amazonaws.com%2Fpublic%2Fimages%2F3adacfb-d32d4-4c09-bd2f-0c75958a2e50_1906x1079.png](https://substackcdn.com/image/fetch/$s_!C6Eg!,f_auto,q_auto:good,fl_progressive:steep/https%3A%2F%2Fsubstack-post-media.s3.amazonaws.com%2Fpublic%2Fimages%2F3adacfb-d32d4-4c09-bd2f-0c75958a2e50_1906x1079.png)



Photo 5: Motorcycle crew training firing from the move at ground targets, with small infantry weapons (Strefa Obroni, 2025)

This change represents a tactical evolution – an adaptation to drone-dominated battlefield, which blurs the line between infantry and cavalry. As Andrii – the same Ukrainian soldier from the aforementioned 3rd Assault Brigade – said in an interview with the newspaper *El Pais*, “such units resemble a form of fast assault light cavalry”. He also described a successful penetration of Ukrainian lines near Pokrovsk in April 2024, using ATVs. This was not an isolated incident: Russian motorcycle and ATV units were officially integrated into offensive operations by mid-2024, with the Russian Ministry of Defence publicly acknowledging their role in offensive efforts and front-line supply operations (El Pais, Ib.).

COMMON TYPES OF MANOEUVRES USED BY MOTORCYCLE ASSAULT GROUPS IN COMBAT

The main types of manoeuvres used by Russian forces in combat are the following:

- a. *simple envelopment* – represents the type of manoeuvre in which motorcycles surround the enemy position from one side to attack from an unexpected direction;
- b. *double envelopment/“pincer” manoeuvre* consists of simultaneous flanking from both sides to overwhelm or encircle the enemy (*photo 6*).
- c. *penetration in depth* involves a rapid advance beyond the first line of defence to disrupt rear area logistics, force rotation/replacement, etc.

- d. *the diversionary manoeuvre* aims to attract the attention of the defending enemy and divert fire away from the main assault force (photo 7).
- e. *reconnaissance by fight* aims to “probe” enemy positions (disposition, combat power, main weapons, reserves, logistics, etc.) while maintaining mobility within the enemy defence device, often testing the defensive reaction and locating weak points.



Photo 6: Double envelopment/“pincer” manoeuvre (Frontelligence Insight, 2025)

Beyond the contact combat in which they engage with Ukrainian forces, the Motorcycle Assault Groups also perform other support roles – they perform limited medical evacuations – extracting the wounded one by one due to space and weight constraints and transporting critical supplies, such as food, water or ammunition, within the load limits of the motorcycles. In offensive operations, these groups have moved forces even inside urban objectives; during the capture of the city of Kurakhove, columns of 3-4 motorcycles rapidly transported small groups of soldiers into the city; ultimately, they rotate individual fighters to/from frontline positions, limited only by the transportation capacity of the motorcycles, but offering a faster alternative to moving on foot or in a vehicle.

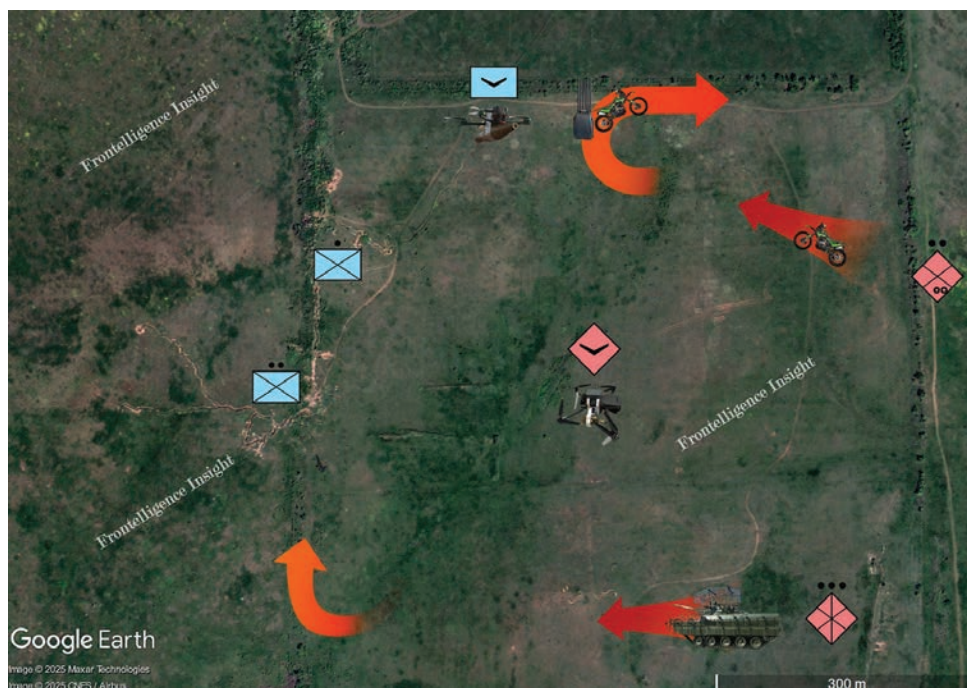


Photo 7: The diversionary manoeuvre (Ib.)

What makes these tactics so effective is the unique combination of speed and decentralisation. Unlike (heavy) armoured tactical vehicles, which carry large numbers of soldiers and are important targets for drones, motorcycles offer a dispersed and fast alternative. Assault Groups – often numbering between a dozen and a hundred bikers – can move quickly over rough terrain, giving drone operators and forward artillery observers (FOs) little time for interception. Furthermore, neutralising a single motorcycle usually requires the same resources as stopping a large armoured tactical vehicle, making them much more cost-effective and tactically elusive.

MOTORCYCLE ASSAULT GROUP TRAINING AND EXERCISES

Although there were no systematic efforts to implement a unified training program within the Russian Army as of early 2024, a number of local initiatives, coordinated at the tactical level, emerged from the bottom up (as innovative solutions). These early efforts resulted in a lack of coordination and consistency. However, by the summer of 2024, the Russian Ministry of Defence initiated measures to formalise training programs for motorcycles and tactical ultra-light all-terrain vehicles (ATVs) in training centres across Russia. In July 2024, during

a visit to a training centre in the Leningrad Military District, Russian Defence Minister Andrei Belousov emphasized the need for dedicated courses for tactical actions on ATVs, buggy-vehicles, and all-terrain motorcycles (Nova News, 2024). He noted their growing role in the rapid supply of ammunition, food, and evacuation of the wounded from combat positions on the front line of defence. Since spring 2025, training of fighters and subunits on all-terrain motorcycles and ultra-light tactical ATV vehicles has been underway both in the ground forces of the Russian Federation and in the occupied territories of Ukraine, integrated training in force groups at the tactical and operational levels. Training usually takes place on improvised or semi-permanent motocross-style tracks designed for motorcycles and other light off-road vehicles. While the quality of these training facilities varies, they tend to have key common features: obstacle courses/tracks simulating minefields, rough terrain, steep climbs and descents (*photo 8*). Training exercises often culminate in the assault phase, in which fighters dismount from motorcycles to attack targets from firing positions or storm simulated enemy trenches and shelters.



Photo 8: Phases during off-road motorcycle training (clockwise) – driving off-road motorcycles in obstacle course, assault exercises with infantry dismounting, training evaluation and driving off-road motorcycles in the complex field (lb.)

Advanced training include UAS/drone team-supported exercises, where instructors simulate enemy FPV drone attacks and evaluate the performance of the strike groups to provide feedback. However, there is limited information on how rigorous these after-action reviews are or how much time is dedicated to correcting deficiencies. The length of the training module varies widely. Basic off-road motorcycle instruction

typically spans at least 16 hours, while more advanced tactical courses – including combat manoeuvres and motorcycle-based assault techniques – can last up to two months. However, in combat conditions, where personnel turnover is high, the full course is rarely feasible. As a result, most trainees likely follow condensed training programs that reportedly last between 2 and 4 weeks.

However, it is important to note that the details of the training/exercises, organisation, and combat performance of these units can vary significantly between formations and large units – and we do not have unified data/information from across the entire front line to provide a definitive, fully data-driven conclusion.

MOTORCYCLE INVENTORY

Given the scale of the war and the demands placed on the Russian Army, a question naturally arises: *Where do the off-road motorcycles come from, what models are used, and Is the Russian Army able to meet its needs with domestic production?* The short answer to the last question is – no. Most of the off-road motorcycles deployed to the front are manufactured abroad, predominantly from China. This comes down to two basic factors: cost and production volume. Although the Russian Defence Sector was developing motorcycles even before the war (and even stepped up its efforts once demand increased), it still fails to meet the needs of the front. Equally important, it seems that the Russian industry is not the only supplier yet. As in the case of drones, motorcycles often reach units through volunteers, local authorities in the unit's home region, personal purchases of servicemen, and state purchases. Given the decentralized supply of motorcycles, the motorcycle fleet of Russian units is remarkably diverse. However, as previously mentioned, Chinese-made off-road models, especially *enduro* motorcycles, are dominant. In June 2025, one of the most common models seen on the battlefield was produced by the Dubai-based company *Sharmax Motors* with production facilities in China. Among the most commonly used are the *Sharmax Sport 280* models from the *enduro* line (*photo 9*), with prices ranging from 180,000 to 300,000 rubles (approximately \$1,900 - \$3,200).

Another emerging alternative, although still less common, is the use of electric motorcycles. These are gaining ground due to several advantages over gasoline-powered models: they are significantly quieter and harder to detect with thermal imaging.

The conflict in Ukraine has made a wider range of lightweight off-road platforms operationally relevant. While motorcycles are effective for rapid and agile troop



Photo 9: The all-terrain motorcycle Sharmax Sport 280 (lb.)

movements, ATVs offer distinct advantages in terms of payload, stability, and off-road capability – occupying a critical niche in the current conflict. Their ability to transport troops, ammunition, equipment, and evacuate the wounded over rough terrain meets urgent operational needs. By the end of 2024, reports indicated that Russian forces were officially training troops in tactical actions with ATVs, signalling their growing tactical importance (*photo 10*). Unlike motorcycles, which excel in speed and range for rapid attacks, ATVs offer greater versatility, supporting a wide range of roles from close-in assault to front-line resupply. Their greater payload and terrain-handling capabilities make them particularly valuable as the logistical backbone of operations conducted under the persistent threat of enemy drones and artillery.

However, while motorcycles and ATVs excel as mobility platforms, they remain ineffective as combat platforms compared to traditional armoured tactical vehicles – rather than acting as traditional cavalry, Motorcycle Assault Groups operate more in dismounted infantry-specific actions. Tanks and traditional armoured tactical vehicles still offer an unmatched advantage. The challenge is not to replace armour, but to rebalance its role within a broader combined arms approach. Motorcycles can allow troops to cross-contested districts or avoid detection, but they cannot replace the brute force and endurance of well-supported mechanised units.



Photo 10: ATVs and buggy-vehicles used by Russian Army in Ukraine (TCH, 2025; Global Defense News, 2025; Global Defense News, 2023)

FEEDBACK IN COMBAT FROM THE UKRAINIAN PERSPECTIVE

Battlefield theories and expectations stemming from tactical experiments often differ from reality. Many Ukrainian military personnel interviewed expressed skepticism about the growing “*emulation*” around off-road motorcycles as a battlefield wonder, emphasising that while off-road motorcycles may be useful in certain conditions, they remain just a platform – far from a transformative innovation.”*Lincoln*” the codename of a Ukrainian tank company commander on the Bakhmut and Chasiv-Yar fronts, assessed the situation on 29 May in the Ukrainian publication “*Censor Net*” – “*They Russians are carrying out assaults with buggies and motorcycles. I can’t imagine how motivated you must be to do this. A conscientious person knows that 90% of them will end up being 200 [military terminology for being killed in action]*”. Another Ukrainian publication specialising in military intelligence – “*Militarnyi*”, concluded that “*it is not clear whether the vulnerability of motorcycles compensates for their use; their speed makes it possible to reduce the time they are in the open, minimizing the possibility of being detected and destroyed. But, despite their speed and manoeuvrability, they are often easy targets for drones and artillery, and due to their lack of protection, their crew members’ chances of survival are minimal*” (Ib.). Numerous videos are circulating on social

networks with motorcycles destroyed by drones, as well as with Motorcycle Assault Groups avoiding explosions more easily than armoured vehicles or SUVs. Andrii, the Ukrainian soldier of the 3rd Assault Brigade, has no doubt that the Ukrainian army should include the use of motorcycles, if not for attacking (the Ukrainians are currently in a defensive position) at least for safer movement to front-line positions. Ukraine maintained its leadership in innovation of war resources until the second half of 2023. The Ukrainian army also adheres to NATO standards, which encourage autonomous decision-making by units, from the company level upwards.

As an assault platform, motorcycles are generally seen as vulnerable and unreliable, rarely delivering decisive results. However, when used in the appropriate role – reconnaissance, fire support (forward artillery observers), support for electronic warfare teams, UAS/drones and armoured vehicles – they can be extremely effective. The challenge, of course, remains execution: Russian forces have struggled to coordinate such combined arms tactical actions even at the company-battalion level, limiting their ability to use motorcycles as effective force multipliers. While more manoeuvrable than traditional armoured tactical vehicles and more effective at evading artillery fire, motorcycles leave pilots exposed and vulnerable to artillery shell fragments. They also offer little protection against FPV drones, which often outrun motorcyclists. Ultimately, casualty rates remain a major concern. Feedback from the front reveals two consistent patterns:

- motorcycle assaults fail to deliver significant tactical results;
- tactical success comes at a high cost, with only one in several assault groups surviving to complete the mission.

This raises serious questions about whether such losses would be considered acceptable by commanders in Western armies. From time to time, the Russian Army's motorcycle assault tactics work – and help motorized infantry regiments advance the front line in eastern Ukraine about a kilometre or so to the west. There is a line of Ukrainian fortifications stretching from the fortress town of Pokrovsk to the ruins of Toretsk, 48 kilometres to the northeast. Capturing Pokrovsk – a major obstacle to Russia's wider advance into the Donetsk region – is likely the top priority. Two Russian armies, each with 10,000 or more soldiers, spent most of last year slowly marching toward Pokrovsk from the devastated town of Avdiivka, 40 kilometres to the southeast, but stalled a few kilometres outside Pokrovsk as Ukrainian resistance stiffened – and Ukrainian drones disrupted supply lines behind the advancing Russian armies. So now the Russians are trying to surround Pokrovsk rather than attack it directly. In recent days, Russian assault groups have stormed a Ukrainian trench line that runs along the T-0504 highway that connects Pokrovsk to

the town of Kostyantynivka, north of Toretsk. Crossing the trench line is a necessary first step if the Russians want to encircle Pokrovsk. At great cost, they are making some progress – and motorcycle assault groups are leading the way. Employing small reconnaissance groups, many of them on motorcycles, the Russians have run into stiff Ukrainian defences, executed by the 14th National Guard Brigade, the 38th Marine Infantry Brigade, and the 117th Mechanised Brigade. Attempting a larger assault on 17 April 2025, Russian forces lost 21 armoured vehicles and up to 240 soldiers (UWG, 2025).

The Ukrainian military has also embraced the Russian concept of Motorcycle Assault Groups. The 425th Assault Separate Regiment announced its first motorcycle assault unit in May 2024, after “*hundreds of hours*” of training, reporting its first successful mission – a night raid in the Kursk region. These developments do not reflect desperate improvisation on the part of either side, but rather a deliberate response to the rapidly evolving threat environment on the modern battlefield.

What is emerging is a new paradigm for *light cavalry* – faster, quieter, more modular, and better adapted to the fast-paced, electronic-engaged operational environment.

SUMMARY AND PERSPECTIVES

To recap, the Russian Army’s Motorcycle Assault Groups are small, fast subunits that use off-road motorcycles for reconnaissance, security, and tactical-level attacks, primarily in military operations in Ukraine, to rapidly penetrate Ukrainian defences and evade (full) drone surveillance, despite the fact that these tactics are described by Ukraine as “*suicide attacks*”. These groups constitute a tactical response to the increased use of drones on the battlefield, providing a mobile platform for reconnaissance and rapid attacks. The deployment of these subunits is a strategic adaptation of the Russian Army to counter the ubiquitous threat of Ukrainian reconnaissance and attack drones.

Key features:

- *small and agile units* – typically consisting of about a dozen to several dozen soldiers;
- *mobility and speed* – off-road motorcycles allow for rapid movement over difficult terrain and rapid infiltration behind enemy lines.
- *allow for evasive tactics* – the speed and manoeuvrability of motorcycles help groups avoid detection and attack by Ukrainian drones.

Tactical role: *reconnaissance – surveillance, security, rapid penetration of enemy lines and small-scale attacks.*

In conclusion, infantry tactics using off-road motorcycles have earned their place and role on the battlefield, but they are unlikely to change the rules of the game on the scale that drones have achieved. However, their use is likely to intensify, in response to current battlefield dynamics. When properly coordinated with other assault elements, these assault groups can enhance operational success and serve as a force multiplier. However, the Russian Army continues to struggle with the synchronisation of combined arms operations at the tactical level, significantly limiting their effectiveness. Internal documents from the Russian Defence Ministry, currently unavailable for publication, suggest that off-road motorcycles, ATVs, and buggy-vehicles will be part of the standard equipment of assault units. These documents also indicate that more than half of the infantry units in some combat units will be equipped with such vehicles to increase mobility. If true, this signals a sustained focus by the Russian military on tactical mobility, a shift that NATO may have to contend with in the event of a direct conflict. As such, this evolving Russian approach deserves further analysis.

This new doctrinal vision, focused on mobility, does not make armour obsolete. Instead, it signifies a rebalancing of combined arms tactics. The most effective tactical actions now tend to combine drones, artillery, and mobile infantry in tightly coordinated attacks. As the Institute for the Study of War (ISW) has noted, the Russian military is *“systematically integrating”* Motorcycle Assault Groups into its planned offensive operations by 2025, as part of a broader shift in tactical thinking – a shift from massed mechanized formations to modular, flexible assault teams that can survive and operate under persistent UAS surveillance and attack (RUSI, 2025).

This development may hold important lessons for NATO and other Western armies. The Turkish military’s 2020 *“Spring Shield”* operation in Syria should have provided an early warning – not least to Russian Army – when coordinated Turkish drone and artillery attacks decimated Syrian armoured units with devastating efficiency and resulted in at least 197 casualties. As military analysts Reynolds and Watling warned in a 2020 article ominously titled *“Your tanks can’t hide,”* survival in the modern battlespace requires layered defensive capabilities – including electronic warfare, radar warning, and short-range air defence (SHORAD) (RUSI, 2020).

Despite these early signals, Western doctrine has been slow to adapt. While defence doctrine reviews and strategic (national) analyses recognise the need for new anti-drone/anti-UAS capabilities and tactics, as well as improved electronic countermeasures, they remain ambiguous about how infantry and armoured units should operate in a drone/UAS-saturated environment. Some tests conducted by the British Army Parachute Regiment in 2021, with electric motorcycles such as

the *Sur-ron Firefly* model (already widely used in Ukraine today), offer compelling advantages in drone warfare: they are quieter and have lower thermal signatures, making them harder to detect (*photo 11*) (Motodeal, 2021).



Photo 11: *Sur-ron Firefly* electric motorcycle tested by the British Army (lb.)

What is emerging is a new paradigm of *light cavalry* – faster, quieter, more modular, and adapted to fast-paced, electronically contested environments. Both Russian and Ukrainian armies are experimenting with and institutionalising these innovations, suggesting that the future of land warfare may belong not just to armoured units or infantry, but to hybrid, networked forces capable of intelligently manoeuvring under constant air threat. Finding the right balance – leveraging the speed and dispersion of light vehicles while maintaining firepower and armour protection – will be essential for survival and victory on the battlefield of the future.

For the Romanian Armed Forces, the implications are clear; the experience of Ukrainian forces, now operating in what is arguably the most technologically dense battlefield in modern history, should serve as a source of urgent tactical intelligence. Most likely, in the event of a potential conflict, the units of the Romanian Armed Forces would operate on the national territory in conditions of an operational environment almost similar to that of the Ukrainian army (geographical, climate, cultural, demographic, technological – *Eastern European Theatre of Operations*). Updating the doctrine, organisation, equipment and training/exercises to reflect this change will be essential if they are to remain operationally effective in future

conflicts. The standard equipment of at least 1/3 of the reconnaissance, FOS, infantry (light, medium, heavy), marine infantry, artillery data assurance, UAS/C-UAS subunits with off-road motorcycles becomes a necessity.

For the Romanian Naval Infantry and its reconnaissance small units, into the conditions of very large and complex area of responsibility (river, delta, lagoon and coastal / littoral), in addition to the AAV-7 amphibious assault vehicles and coastal patrol boats, motorcycles are essential in achieving mobility in the lagoon area (the inner land sector and on the lagoon sandy strip from Sf. Gheorghe to Vadu), on the delta sand islands and on the river banks – as follows:

- mobility of research-surveillance subunits (land and with UAS/drones) through patrol;
- counter-reconnaissance (neutralisation of enemy scouts and their systems that have penetrated the national territory);
- support for the installation / operation of information collection systems (land sensors/GSR, portable electronic warfare systems, etc.);
- mobility of forward artillery observer teams (land artillery and river naval artillery) or JTAC (forward tactical air control teams);
- mobility of marine infantry subunits for control of the banks and port areas.

Transportation of motorcycles during deployment (on the lake/river) in the border sectors would be carried out with light boats and river vessels, given the small dimensions of the motorcycles. Also, in the case of long-term tactical actions (3-7 days) in isolation conditions, fuel resupply (batteries in the case of electric motorcycles) would be easily achieved, using both military river boats on the standard logistics chain but also civilian boats or by parachuting / helicopter launch.

BIBLIOGRAPHICAL RESOURCES:

1. Bussines Insider (2025), <https://www.businessinsider.com/ukraine-motorcycle-assault-rifle-war-russia-off-road-2025-5>, retrieved on 11 August 2025.
2. El Pais (2024), <https://english.elpais.com/international/2024-06-18/russian-army-develops-motorcycle-assault-units-to-carry-out-lightning-attacks-on-the-front-lines.html>, retrieved on 21 August 2025.
3. Frontelligence Insight (2025), <https://frontelligence.substack.com/p/21st-century-dragoons-dissecting>, retrieved on 2 August 2025.
4. Global Defense News (2023), <https://armyrecognition.com/focus-analysis-conflicts/army/conflicts-in-the-world/russia-ukraine-war-2022/russia-deploys-a-new-atv-is-deployed-to-bolster-troops-on-the-ukrainian-frontline>, retrieved on 21 July 2025.
5. Global Defense News (2025), <https://www.armyrecognition.com/archives/archives-land-defense/land-defense-2024/russian-army-views-new-plastun-tt-articulated-atv-as-replacement-for-chinese-desertcross-in-ukraine?highlight=WyJydXNzaWEiXQ==>, retrieved on 21 August 2025.

6. McGovern, D. (21 August 2025). *Drones Drive Battlefield Motorcycle Tactical Shift*, Royal United Services Institute (RUSI), <https://www.rusi.org/explore-our-research/publications/commentary/drones-drive-battlefield-motorcycle-tactical-shift>, retrieved on 21 August 2025.
7. Motodeal (2021), <https://www.motodeal.com.ph/articles/motorcycle-news-philippines/british-army-begins-testing-electric-motorcycles-paratroopers>, retrieved on 17 September 2025.
8. Nova News (2024), <https://www.agenzianova.com/ro/news/Ministrul-rus-al-ap%C4%83r%C4%83rii-inspecteaz%C4%83-o-tab%C4%83r%C4%83-de-antrenament-din-districtul-Leningrad/>, retrieved on 21 August 2025.
9. RUSI (2020), <https://www.rusi.org/explore-our-research/publications/rusi-defence-systems/your-tanks-cannot-hide>, retrieved on 12 August 2025.
10. RUSI (2025), <https://www.rusi.org/explore-our-research/publications/commentary/drones-drive-battlefield-motorcycle-tactical-shift>, retrieved on 12 August 2025.
11. Segura, C. (18 June 2024). Russian army develops motorcycle assault units to carry out lightning attacks on the front lines, El Pais International, <https://english.elpais.com/international/2024-06-18/russian-army-develops-motorcycle-assault-units-to-carry-out-lightning-attacks-on-the-front-lines.html>, retrieved on 21 August 2025.
12. Strefa Obroni (2025), <https://strefaobrony.pl/200-tysiecy-motocykli-z-chin-trafi-na-front-rosja-rozszerza-nowa-taktyke/ar/c1p2-27743991>, retrieved on 20 August 2025.
13. TCH (2025), <https://tsn.ua/en/ato/russian-offensive-in-sumy-region-enemy-sabotage-groups-breach-border-on-atvs-2834168.html>, retrieved on 21 August 2025.
14. Telegraph (2024), <https://www.telegraph.co.uk/world-news/2024/06/03/russian-troops-modify-motorbikes-with-anti-drone-cages/>, retrieved on 21 August 2025.
15. The British Army begins testing electric motorcycles for paratroopers – The Sur Ron Light Bee is a formidable electric dirtbike, Motodeal (27 December 2021), <https://www.motodeal.com.ph/articles/motorcycle-news-philippines/british-army-begins-testing-electric-motorcycles-paratroopers>, retrieved on 12 September 2025.
16. United 24 Media (2024), <https://united24media.com/war-in-ukraine/inside-ukraines-rapid-counteroffensive-in-dobropillia-before-facing-russias-meatgrinder-in-pokrovsk-14020>, retrieved on 14 September 2025.
17. UWG (2025), <https://uavarta.org/en/war-in-ukraine-today-latest-news-17-april-2025-photo/>, retrieved on 11 August 2025.
18. *21st Century Dragoons*: Dissecting Russia's Motorcycle Assault Tactics, Frontelligence Insight (23 June 2025), <https://frontelligence.substack.com/p/21st-century-dragoons-dissecting>, retrieved on 17 September 2025.
19. <https://english.elpais.com/international/2024-06-18/russian-army-develops-motorcycle-assault-units-to-carry-out-lightning-attacks-on-the-front-lines.html>, retrieved on 17 September 2025.

BUILDING UP A PROSPECTIVE STUDY FOR THE WORLD OF TOMORROW

Professor Dr. Iulian CHIFU

Centre for Conflict Prevention and Early Warning, Bucharest

DOI: 10.55535/RMT.2025.3.13

Prospective studies, avoiding strategic surprise and anticipating the evolutions, are the aspiration of a number of methodologies. Our article aims to make a reason and find the main factors that would influence the reassessment of the World Order of tomorrow based on a Romanian methodology of prospective studies. The level of ambition is to separate the continuity versus the dramatic change and to find the critical indicators that are drawing the scenarios of the future, be they those of continuity, of discontinuity and black swan cases. Relative certainties are helping us draft the black swan scenarios of highly improbable but also enormous impact. The results and conclusions are bringing to the forefront both technology and malaises of democracy, together with a militaristic epoch where the chance is to avoid kinetic wars through mitigations and coping with the rivalries and power shifts in geopolitical capacity.

Keywords: prospective studies; critical uncertainties; relative certainties; continuity; change;

METHODOLOGICAL BACKGROUND

In order to avoid exposing the most important institutions and decision makers to the consequences of strategic surprise (Cancian, 2018), we have introduced the Romanian methodology of prospective studies in 2012 (Chifu-2, 2015; 2016, pp. 75-113). This phenomenon means that an institution is not able to anticipate, to prevent, and to react properly to a crisis of the amplitude to produce the disruption of the activity of an institution, a government, or a state. The level of resilience proves to be very low in such conditions. Moreover, to cope with such a crisis, the decision-making system has to react on an ad-hoc basis, without preparation or proper instruments and anticipation, including in communication in due time and proper manner to its own public, with major consequences for citizens' security and their lives, and exposing the decision-maker to public opprobrium (Chifu-5, 2023).

We have developed the prospective studies methodology based on a technique used by the Dutch intelligence services – PLATO (Schinkel, 2013; Chifu-2) – *plausible tomorrows*, that we have completed, experimented and used in several cases to identify alternative scenarios for a critical evolution in international relations and security studies. We have developed as well several times the methodology related to Ukraine (Chifu-1, 2014; Chifu, Nantoi, Getmanchuk, 2015; Chifu-3, 2015), the Black Sea Region (Chifu, Bălăsoiu, 2018) and the evolution of international relations (Chifu-5).

Our study has several steps to be accomplished, each and every one inseparable from the final outcome. The first is an assessment of the situation at the moment we begin the analysis, updated at the end of the process. The second goes into identifying the evolutions that are affecting our explored evolution of the situation of the world. The third is extracted from the brainstorming part of the different influences on a short, medium, and long term, the critical indicators, in a complete and non-contradictorily system. The fourth is identifying relative certainties and critical uncertainties linked to the required process and is aimed at identifying the New World Order reassessment. The fifth is creating the scenarios by combining the different possible values of the independent indicators identified in each system for the time frame analysed. And the sixth deals with playing the selected scenarios.

We have developed the assessment considering four domains of concerns:

ACTORS

We have focussed on Russia, Ukraine, the EU, the USA, NATO, and China, even though we have assessed that, in the new technological world, each country that possesses new technology or resources of any kind linked with such a technology could play a bigger role than that recommended by its economy, research, military, political, and international relevance (Chifu-5). But this is for the future. The initial assessment is focusing on existing big actors, relevant actors, capable of disruption in the world order, or having a say in remodelling this order (Rogers, 2019).

RELATIONS

We have focused on the most important bilateral relations linking the big relevant players: EU-USA, Russia-China, USA-Russia (discussing also some convergent visions of Putin and Trump), EU-Russia, EU-China, USA-China. Once again, other actors or relations could influence the evolution and enter the relevant stage, in the future, but at the initial moment of analysis, the assessment focuses on the existent ones (Oxford Analytica, 2013).

WARS, CONFLICTS, CONFRONTATIONS

The conflicts, wars, and confrontations are indispensable to the original assessment and to the evolution of the World Order (Ramsbotham, Woodhouse, Miall, 2011). We have focused on Russia's war of aggression against Ukraine, on the Israel/USA confrontation with Iran, on the conflict in the Middle East and its possible outcomes, on the USA-China economic and possible military rivalry falling into a possible conflict on Taiwan or in the Indo-Pacific region, as well on the Russia-Europe/NATO(USA?) possible rivalry or confrontation (Walpole, 2012).

DRAMATIC CHANGES

There are signals of developments that can affect the international World Order through dramatic changes and ruptures in the continuity of today's life (Gowing, Langdon, 2018). We have identified here the technology as an agent of dramatic changes, its impact, and the independent evolution of the human society, a disruptive global crisis/civil emergency like the pandemic, and the war (full scale-war, quasi-global war).

During our study, we organised nine brainstorming sessions with different groups of some 50 experts of different ages and master degree students to absorb fresh ideas. The subjects are the result of the analysis on the dynamics of the international world order and what could prompt dramatic changes issued via

the trends developed in areas with high impact. We explored in those brainstorming sessions:

- The impact of the war in Ukraine on the regional and global security architecture.
- The EU-Europe relationship and review of the strategic commitments.
- Hybrid threats, disinformation and cyber security impact on the world of tomorrow.
- China's raise and the consequences on the global geopolitical environment.
- NATO's provocations and opportunities.
- Perspectives of European's strategic autonomy.
- Energy security, dependency of external resources, and its impact on the elections and reassessment of the World Order of tomorrow.
- The future of defence policies – options and scenarios.
- The information-cognitive warfare and its level of impact on the evolution of the world tomorrow.

RELATIVE CERTAINTIES, CRITICAL UNCERTAINTIES

Relative certainties are the facts that 100% of the experts would claim as true. We used the relative certainties in order to identify and to play *black swan* (Taleb, 2010) scenarios, with low probability and high impact. We identified ten relative certainties, with the time frame coming from short (s), medium (m), and long (l) term, or all meaning for all time frames considered (all):

- s+m – Putin maintains the power, in spite of the natural age, health problems and rivalries inside the system;
- all – Russia will avoid using a nuclear bomb. The consequences are already established and could come with high costs and loss of partners and support;
- s+m – Russia will maintain maximalist requests in the war with Ukraine due to the revisionist posture and the veto demand for the security in Europe;
- all – Russia wants to revive its posture of superpower recognised at the global level;
- all – the war in Ukraine will not create precedents for a new world order, meaning specifically that Ukraine will not accept a trade, territories versus peace. In this case, Ukraine, a conventional power, can prove that it can resist a nuclear actor, Russia, in a conventional war, creating a precedent. Ukraine, a smaller actor, but more flexible, adaptable and inventive, resists or even can win the war with Russia when it is about avoiding to meet

the level of ambition of Putin's Russia, meaning occupying Ukraine, changing the legitimate government elected, and depriving it of its armed forces and capacities to defend itself, questioning the very identity and right to exist as a state;

- s+m – Europe will fight for the rules-based order and defend them. In such a way, we are considering a continuity, with the EU and its member states being status quo powers;
- all – China will challenge US global power;
- all – China with its allies will challenge the World Order rules and introduce revisionist demands altering rules-based order.
- s+m – The world is sliding towards authoritarianism. Democracy indexes fall in the interest of the world, a fact already proved by the last situation evaluated for freedom of expression, media freedom, exercise of human rights at a global level, with indexes on the fall;
- s – Russia will continue the war or a war at any costs and will require a veto on security of Europe.

Critical uncertainties – the same way as in the case of relative certainties, the critical uncertainties are related to the facts and evolutions that are game changers, dramatically changing the evolution of the world tomorrow (Cortney, Kirklnad, Viguerie, 1997). In those cases, we also used the brainstorming sessions and the expert sessions determined the following critical uncertainties for short, medium and long terms:

- m+l – Russia will continue the war at all costs and request for veto on security of Europe or, on the contrary, will stop the war in some clear conditions. Even though it is a relative certainty in the short run, in the medium and long term, it becomes a critical uncertainty coming from the economy and Putin's own relations with the public and instruments of power in the Kremlin;
- m+l – here the stakes are coming from the forces involved in splitting Europe versus the ones that create a higher convergence because of the new common enemy, Russia. In that case, the EU can affirm itself as a global relevant actor;
- s+m – enemy within the gates: nationalism/sovereign-ism, MAGA export of system in Europe and the world are changing dramatically the political landscape, challenging the rules and relations. Alternatively, this anti-system,

populist rhetoric becomes an extinguished fashion with the opposition of Europeans or when Trump changes its position or leaves office without a MAGA successor in place;

- all – the militaristic age: we are moving towards a global war, at least in the form of a full-spectrum warfare with some kinetic regional wars, or, on the contrary, people cope and mitigate wars and conflicts, maintaining them in a clear, limited framework, without harsh consequences;
- all – three evolutions are related to Europe/the EU: first, Europe and the USA continue to form a strong democratic alliance, limiting their differences; second, the USA and Russia, together with the nationalist-sovereign-ist supported movements, are dismantling Europe/the EU in nation states; and third, the USA and China will fight, through excessive charm and constrains instruments, for the EU/Europe's support in their own program and design of the world order;
- m+I – technological dramatic impact: the first choice is technology destroying or leading to the meltdown of the human society (just individuals, not believing anything), in a world dominated by machines and algorithms; the second would be the survival and adaptation of the human race to technology, with a substantial number of people left behind; and third choice, a complete techno-human new integrated world, with the dominance and control of the human on the technologies that they invented.

Critical indicators

Based on the critical uncertainties identified (Trung Anh, 2002), we have established the system of critical indicator for the short, medium and long term, as follows:

Short-term (6-12 month) indicators:

1. Enemy within democratic states: nationalism/sovereign-ism, MAGA export of system in Europe and the world would alter the democratic system in Europe itself. Or, alternatively, the fashion of those populism/nationalism approaches will be extinguished, will pass.

2. Militaristic age: the world enters into a militaristic age, prone to conflicts, a global war/full spectrum warfare as a rule, with Russian episodes of kinetic wars, full-scale, high-intensity, long-term wars of attrition. Or the steam will cease and the confrontation will be extinguished due to the lack of means, money, people, will, or due to the increase of vigilance, preparedness, and resilience from the people.

3. The US role in Europe: the EU/Europe-USA democratic alliance or USA-Russia plus nationalist movements dismantling Europe-EU in nation states or USA-China will fight for EU-Europe's support in their own programs.

4. Ukraine will resist/Ukraine will fail (through a domino effect after a breach in the first line).

5. EU will support Ukraine in the long run/stop financing Ukraine, block support.

So, for the short term, we have identified, through different combinations of the value of the critical indicators, **48 scenarios** (2x2x3x2x2 values for indicators). We add to that the **ten "black swan" scenarios**.

Medium-term (3-5 years)

1. Russia in the war: Russia will continue the war at all costs and require a veto on the security of Europe or Russia will stop the war due to economic shortages, discontent of the society with taking social and development resources for feeding the war.

2. The EU global actor: We will have a split EU or the convergence of the member states even further due to a common enemy, making the EU a global actor, relevant in the new World Order dynamics.

3. The world enters into a **militaristic age**, prone to conflicts, a global war/full-spectrum warfare as a rule, with Russian episodes of kinetic wars, full-scale, high-intensity, long-term wars of attrition. Or the steam will cease and the **confrontation will be extinguished** due to the lack of means, money, people, will. Or increase of vigilance and resilience from the people.

4. The EU will support Ukraine in the long run, EU-Ukraine will mark a convergence in security and defence with Europe becoming a global geopolitical actor, **or the EU will stop financing Ukraine, block support.**

Here we have **16 scenarios** (2x2x2x2 values for indicators) and just **nine "black swan" scenarios**.

Long-term (10-15 years)

1. The EU global actor: We will have a split EU or the convergence of the member states even further due to a common enemy, making the EU a global actor, relevant in the new World Order dynamics.

2. The world enters into a **militaristic age**, prone to conflicts, a global war/full-spectrum warfare as a rule, with Russian episodes of kinetic wars, full-scale,

high-intensity, long-term wars of attrition. Or the steam will cease and the **confrontation will be extinguished** due to the lack of means, money, people, will. Or increase of vigilance and resilience from the people.

3. Technological impact: The first choice is technology destroying or leading to the meltdown of the human society (just individuals, not believing anything), in a world dominated by machines and algorithms; the second would be the survival and adaptation of the human race to technology, with a substantial number of people left behind; and the third choice, a complete techno-human new integrated world, with the dominance and control of the human on the technologies that they invented (Chifu, Savu, 2020; Chifu-4, 2021, pp. 13-22).

4. USA-China rivalry: confrontation or cohabitation. Globalization or split into globalised blocks.

Here we have **24 scenarios (2x2x3x2 values for indicators)** and **five “black swan” scenarios to play.**

SCENARIOS TO BE PLAYED:

Based on the critical indicators, we have established the scenarios to be played in the study, and we stick to the best case, worse case and most probable case (Manning, 2012) for each of the three time-frames – short, medium and long term. We added a special case of debate on the technological impact, meaning the scenarios that put technology as a dramatic game changer¹, which is leading the evolution of the World Order, and we are not talking here about supply chains (Grabo, 2002), but about the impact on humankind and human society (Chifu, Savu, ib.), as well as the relevance in dominance of the world. We added to that the ten “black swan” scenarios, as follows:

Short-term (6-12 month):

- *best case (continuity):* enemy within will fall, Ukraine succeeds, the EU supports Ukraine, US constructive/supportive role in the EU, responsible transfer of defence attributions from the USA to Europe (Europe meaning European NATO leg, EU or the coalition of the willing), and managing global rivalries without kinetic full-scale war;

¹ See Ministry of Defence, *Strategic Trends Programme, Global Strategic Trends out to 2040*, fourth edition, Development, Concepts and Doctrine Centre (DCDC), UK, 2010; NIC, *Global Trends 2030*.

- *worst case (dramatic change)*: enemy within will prevail in a number of states, that will change the European Union in an intergovernmental weak union, the USA will retreat without considering lack of capabilities of the EU, the EU will drop the support for Ukraine which will implode/domino reaction, militarism will grow towards a war confrontation;
- *most probable case (transformation)*: changes in some states, but maintaining the course for the EU, support for Ukraine, Ukraine resisting, US responsible transfer to the EU and support (diminished), difficult managing USA-China, USA-EU, trade and rare earth issues, USA-Russia, EU-Russia relations, war sends signals in Europe/NATO engaging those states, new confrontations emerged or accentuate in the Middle East, Indo-Pacific. No war, no peace.

Medium-term (3-5 years):

- *best case (continuity)*: Russia will stop the war, costs and economic problems, a way out. The EU global actor, reinforced, and solidarity between states. Conflicts will be kept out of explosion in kinetic wars. The EU will support Ukraine;
- *worst case (dramatic change)*: Russia will continue the war. The EU will review its functioning into a more intergovernmental body, challenged in the European Council by a growing number of states, including France/Germany with populist extreme right inputs. Emergence of militaristic war-prone world. The EU will stop supporting Ukraine, and Ukraine will resist only due to a few states/coalition of the willing;
- *most probable case (transformation)*: Russia will continue the war. The EU will navigate its way between blockages from several states and the need to reinforce its global stance. The EU will continue supporting Ukraine, but diminishing its footprint. The EU will consolidate its position at a global level. War-prone world, militaristic approach, without a real explosion of new conflicts and efforts to keep the existing ones under control.

Long-term (10-15 years):

- *best case (continuity)*: the EU global actor, with a rising relevance at the global level, building a military might and strong deterrent. The USA-China rivalry is manageable, without huge frictions, managing existing and emerging conflicts at the global level. Reassessment of the international

World Order in a stable, convened way. Integration man-machine/algorithms and absorption of technological evolution;

- *worst case (dramatic change)*: the EU is irrelevant, formal, losing its presence and influence at the international level. Militaristic approach and a long range of conflicts that involve the West, including Russia-NATO on article 5 basis. The USA-China rivalry moving to war in Indo-Pacific/Taiwan and nuclear sabre-rattling in the public space. Splits inside the society, technology playing an important and individual self-conscious role in security, defence and day-by-day evolutions;
- *most probable case (transformation)*: The EU aims to become a global actor, has added military might, but is still kept away by countries with Eurosceptic leadership blocking the functionality and the Qualified majority decisions. The USA-China rivalry has episodes and ups and down, including clashes in the Indo-Pacific and split of globalization into two parties, with a number of exceptions and communication still on, dollarization continuing to be the reference for the exchanges between the blocks. Militarism and using wars to solve disputes is more present, even though not between the Big Power actors, that tend to manage the kinetic confrontation and nuclear rivalries. Humans will survive, adapt, and some part of the people will be left behind by the accelerated technological changes.

plus **technological case debate**:

- Scenario where technology takes over the core of the debate and becomes the most important factor of the world in the long run.

Ten “black swan” scenarios

The ten “*black swan*” scenarios, with high impact and low probability, are made by challenging the relative certainties:

- s+m – Putin maintains power, in spite of the natural age, health problems and rivalries inside the system;
- all – Russia will avoid using a nuclear bomb. The consequences are already established and could come with high costs and lost of partners and support;
- s+m – Russia will maintain maximalist requests in the war with Ukraine due to the revisionist posture and the veto demand for the security in Europe;
- all – Russia wants to revive its posture of superpower recognised at the global level;

- all – the war in Ukraine will not create precedents for a new world order, meaning specifically that Ukraine will not accept a trade, territories versus peace. In this case, Ukraine, a conventional power, can prove that it can resist a nuclear actor, Russia, in a conventional war, creating a precedent. Ukraine, a smaller actor, but more flexible, adaptable and inventive, resists or even can win the war with Russia when it is about avoiding to meet the level of ambition of Putin's Russia, meaning occupying Ukraine, changing the legitimate government elected and depriving it of its armed forces and capacities to defend itself, questioning the very identity and right to exist as a state;
- s+m – Europe will fight for the rules-based order and defend them. In such a way, we are considering a continuity, with the EU and its member states being status quo powers;
- all – China will challenge US global power;
- all – China with its allies will challenge the World Order rules and introduce revisionist demands altering rules-based order;
- s+m – the world is sliding towards authoritarianism. Democracy indexes fall in the interest of the world, a fact already proved by the last situation evaluated for freedom of expression, media freedom, exercise of human rights at a global level, with indexes on the fall;
- s – Russia will continue the war or a war at any costs and will require a veto on security of Europe.

In total we had 20 scenarios played from a total of 112 possible – 88 scenarios from indicators and 24 “black swan” scenarios.

CONCLUSIONS

After playing all the scenarios, we have realised that a number of conclusions are imposing themselves and are going to be definitory for the future of the World Order, that of the EU/Europe as a global actor and the future of humanity.

First, technology is going to play a more important role, even critical in some cases, for the future of the World Order, provided that the humanity can begin to adapt to this future right now, in the short and medium terms, as soon as possible, for avoiding the negative possible trends completely splitting the humanity and society into individuals included in cognitive tribes or letting a big part of the humanity behind, into a level of illiteracy for the new technology that is preventing the integration with machines and algorithms.

Second, the so-called **enemy within the democratic societies, that are derailing the rules and channelling them towards autocratic forms of governance** where power, physical and technological, plays the most important role, is going to define the world of tomorrow and the role of the EU/Europe as a global actor or the inclination to isolate communities inside nation-states, prone to disinformation warfare that shape free choices, tastes and way of life, altering liberty and human rights.

Third, historians are telling us that **any change of high tectonicity between the substance and form of the World Order is coming after a war**, a kinetic confrontation at the global level. It depends on the humankind and its leadership if that could stay in the full spectrum warfare without kinetic full-scale war or we will repeat the history of the past, destroying parts of our heritage, buildings, humans and diversity.

BIBLIOGRAPHY:

1. Cancian M. F. (2018). *Avoiding coping with surprise in Great Power Conflicts*, 2018, Center for Strategic and International Studies (CSIS), www.jstor.com/stable/resrep22428.8, retrieved on 22 July 2025.
2. Chifu, I.-1 (2014). *Prospectives on Ukraine Crisis. Scenarios for a mid-long term evolution*. București: Editura Institutului de Științe Politice și Relații Internaționale al Academiei Române.
3. Chifu, I.-2 (2015). *Prospective studies: a Romanian Methodology. Ukraine as a case study in Scenarios for a Short-Mid-Long-Term Evolution*, in *New Approaches in Social and Humanistic Sciences*, September 11-13, 2015, Chișinău, Republic of Moldova, Working Papers, International Conference, Lumen Media Publishing UK, 2016, Iași, pp. 75-113.
4. Chifu, I.-3 (2015). *Prospective Analysis of Ukrainian Crisis: Scenarios for mid-long term evolution*, *Ukraine Analytica*, No.1/9 October 2015, Odessa.
5. Chifu, I.-4 (2021). *Securitatea tehnologică. Un nou domeniu de strictă actualitate a securității viitorului*, in *Infosfera*, no. 2/2021.
6. Chifu, I.-5 (2023). *Studii prospective și metodologii alternative, în eșafodajul de securitate din secolul 21*, Vol. 4 from *Reconfigurarea securității și a Relațiilor Internaționale în Secolul 21*. București: RAO Publishing.
7. Chifu, I.-6 (n.d.). *Studii prospective și metodologii alternative, în eșafodajul de securitate din secolul 21*.
8. Chifu, I., Bălăsoiu, N. (2018). *Prospective studies of the Wider Black Sea Region. Scenarios for its future in times of high international turbulence*. București: Editura Institutului de Științe Politice și Relații Internaționale "Ion I.C. Brătianu" al Academiei Române.

9. Chifu I., Nantoi, O., Getmanchuk, A. (2015). *Prospective on Ukraine Crisis. A trilateral approach*. București: Editura Institutului de Științe Politice și Relații Internaționale "Ion I.C. Brătianu" al Academiei Române.
10. Chifu, I., Savu, L. (2020). *The Impact of Technology on Human Being, Society and Politics*. București: Editura Institutului de Științe Politice și Relații Internaționale "Ion I.C. Brătianu" al Academiei Române.
11. 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 August 2025.
12. Gowing, N., Langdon, C. (2018). *Thinking the unthinkable: a new imperative for leadership in the digital age*, John Catt Educational Ltd, 2018, ISBN 978-1911382744, 202 p.
13. Grabo, C.M. (2002). *Anticipating Surprise. Analysis for Strategic Warning*. Center for Strategic Intelligence Research, Joint Military Intelligence College, 2002, ISBN 0-9656195-6-7, 175 p, http://www.ni-u.edu/ni_press/pdf/Anticipating_Surprise_Analysis.pdf, retrieved on 22 August 2025.
14. Manning, R.A. (2012). *ENVISIONING 2030: US Strategy for a Post-Western World*. A report of the Strategic Foresight Initiative at the Brent Scowcroft Center on International Security, Atlantic Council, Washington D.C., <https://www.atlanticcouncil.org/in-depth-research-reports/report/envisioning-2030-us-strategyfor-a-postwestern-world/>, retrieved on 12 August 2025.
15. Ministry of Defense (2010). *Strategic Trends Programme, Global Strategic Trends out to 2040*, fourth edition, Development, Concepts and Doctrine Centre (DCDC), UK, 2010; NIC, Global Trends 2030.
16. *Predictions have key limits in global risk assessment*, Oxford Analytica, Thursday, May 16 2013, at <https://dailybrief.oxan.com/Analysis/DB183360/Predictions-have-key-limits-in-global-risk-assessment>, retrieved on 12 August 2025.
17. Ramsbotham, O., Woodhouse, T., Miall, H. (2011). *Contemporary conflict resolution. The prevention, management and transformation of deadly conflicts*, 3rd ed., Polity Press, Cambridge.
18. Rogers, J. (2019). *Audit of Geopolitical Capability. An assessment of 20 major powers*. Henry Jackson Society, ISBN: 978-1-909035-50-8, 64 p., <https://henryjacksonsociety.org/wp-content/uploads/2019/01/HJS-2019-Audit-of-Geopolitical-Capability-Report-web.pdf>, retrieved on 22 August 2025.
19. Schinkel Marjaand Blum, D. (2013). Presentation at the GFF-Global Future Forum conference, in the building of the Scottish Government conference entitled "Developing the conceptual framework for International Foresight Analysis", Glasgow, Scotland.
20. Taleb, N.N. (2010). *The Black Swan. The Impact of the Highly Improbable*, Random House.
21. Trung Anh, D. (2002). *Known Knowns, Unknown Knowns, and Unknown Unknowns What you know and what you don't?*, Data Driven Investor, 2002, <https://medium>.

com/datadriveninvestor/known-knowns-unknown-knowns-and-unknown-unknowns-b35013fb350d, retrieved on 22 August 2025.

22. 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, 250 p.

THE EUROPEAN UNION'S STRATEGIC APPROACH TO THE BLACK SEA REGION – IMPLICATIONS FOR REGIONAL SECURITY AND THE ROLE OF ROMANIA –

Dr. Violeta NICOLESCU

Ministry of National Defence, Defence Policy Directorate

DOI: 10.55535/RMT.2025.3.14

The European Union's Strategic Approach to the Black Sea Region marks a defining stage in the evolution of the European Union's foreign and security policy. The document reflects a paradigm shift, whereby the Black Sea is no longer perceived as a geopolitical periphery, but as a central strategic space for the security, stability and prosperity of Europe. The context for the development of the strategy is determined by the war of aggression launched by the Russian Federation against Ukraine in February 2022, the intensification of maritime and hybrid threats, as well as the process of the Union's enlargement to the East. The new strategy, structured on three pillars – security and resilience, sustainable growth and environmental protection – provides an integrated framework for collective action. For Romania, the document creates opportunities to consolidate its role in the region and to actively engage in the European security architecture in the Black Sea.

Keywords: Black Sea; strategy; maritime security; critical infrastructure protection; connectivity;

INTRODUCTORY CONTEXT

The European Union Strategic Approach to the Black Sea Region issued in May 2025 represents an essential landmark in the foreign and security policy of the European Union. This document comes against the backdrop of profound changes in the geopolitical architecture of Eastern Europe, the intensification of threats to maritime and energy security, and the need to transform the Black Sea region into a stable, secure, and prosperous space. A number of factors underlie the EU's decision to issue such a strategic document – long awaited by the EU Member States in Eastern Europe, especially those bordering the Black Sea.

Thus, the most important factor influencing the development of this strategy is the *Russian Federation's war of aggression against Ukraine*, which began in February 2022 and is still ongoing in 2025. The Black Sea has become, in part, a *theatre of war*, Russia using it for naval blockades, sea-launched missile attacks, sabotage operations, and threats to Ukraine's trade and export routes. Civil navigation has been seriously affected, including by attacks on port infrastructure in Odessa, Chornomorsk and Izmail, located very close to the border with Romania – a state that is also facing (M.Ap.N., 2025) airspace violations by drones or drone fragments falling in border towns. Also, the *massive militarization of the region* by Russia, including in the Crimean Peninsula occupied in 2014, has created a *security gap* perceived by the EU as a strategic threat to the entire eastern region. Thus, the High Representative of the European Union for Foreign Affairs and Security Policy, Kaja Kallas, explicitly emphasized that *"the security of the Black Sea is also vital for the security of Europe"*¹.

Another factor that determined the creation of the document lies in the *need for strategic coherence and joint action at EU level*. Until 2025, European approaches to the Black Sea region were fragmented, sectoral and, often, reactive. EU Member States in the region – notably Romania and Bulgaria – have repeatedly called for an integrated European strategy for the Black Sea, including in the context of the adoption of the new EU Strategic Compass (2022). Previously, in the first half of 2019, the Romanian Presidency of the Council of the EU focused on promoting regional cooperation in the Black Sea region, with the support of the

¹ *Black Sea Strategy: Press remarks by the High Representative of the Union for Foreign Affairs and Security Policy/ Vice-President of the European Commission, Kaja Kallas*, 28 May 2025, https://www.eeas.europa.eu/eeas/black-sea-strategy-press-remarks-high-representativevice-president-kaja-kallas_en, retrieved on 10 September 2025.

European Union. The most notable result of this period was the adoption in the same year of two framework documents: the *Common Maritime Agenda for the Black Sea* (Ministerial Declaration on a Common Maritime Agenda for the Black Sea, 2019) and the *Strategic Black Sea Research and Innovation Agenda* (Black Sea Strategic Research and Innovation Agenda, 2019), both subsumed under the Black Sea Synergy. Also, previous instruments, such as the Black Sea Synergy (Black Sea Synergy – A New Regional Cooperation Initiative, 2007) or regional cooperation projects with the Eastern Partnership (EaP) countries, did not provide a unifying strategic vision. In fact, the EU Strategic Approach to the Black Sea is built on the Black Sea Synergy, the latest implementation report (Black Sea Synergy: 4th review of a regional cooperation initiative – period 2019-2023, 2024) being published on 3 July 2024 and covering the period 2019-2023. In light of the above, the unstable context in the region has imposed the need for coordinated collective action to ensure not only security, but also economic development, connectivity and environmental sustainability. Thus, the May 2025 strategy responds to the need to position the Black Sea as a central strategic area in the EU's foreign, energy and defence policy.

Another key element that determined the development of this strategy is the *EU's enlargement process to the east*, with a focus on supporting Ukraine and Moldova in their reconstruction and integration. Thus, Ukraine and the Republic of Moldova have been official candidates for EU membership since 2022 (European Council meeting Conclusions, 2022), and accession negotiations are ongoing. In this logic and in relation to the regional security context, attention is focused both on the reconstruction of Ukraine and its integration into the single market – which requires modern infrastructure, access to transport and energy corridors, and secure maritime connectivity, as well as on the Republic of Moldova which, as a landlocked state, depends on access to Romanian and Ukrainian ports for trade and essential imports. Therefore, a *strategic approach at regional level* is essential to avoid fragmentation of support and to contribute to the success of the European integration process in the Wider Black Sea Region.

In addition, multiple crises (energy, climate, migration, infrastructure) have also had their say, with the Black Sea also becoming a nodal point for several interconnected crises: the post-2022 energy crisis that forced the EU to seek alternative corridors for gas and electricity; climate change and excessive pollution that threaten biodiversity and the quality of life in coastal areas; migration from the Caucasus and the Middle East, intensified by regional instability, affecting sea routes and ports on the Black Sea. In this context, the strategy issued in May 2025 proposes not only security measures, but also structural measures for climate change adaptation, sustainable development and civil protection, in a coherent and long-term manner.

Last but not least, the adoption of the strategy also reflects the *unity and solidarity between the Member States* within the Union. Romania and Bulgaria, Member States directly affected, have consistently called for a more applied focus on Black Sea policies. The Baltic countries and Poland have also supported this approach, seeing a direct connection between Black Sea security and Baltic Sea security. By connecting the two areas, the Commission also saw in this approach an opportunity to demonstrate the EU's internal cohesion and its capacity to react at a difficult time for the neighbourhood policy.

Thus, the EU Strategic Approach to the Black Sea did not emerge in isolation, but is the result of cumulative geopolitical, security and economic pressures, accentuated by the war in Ukraine, climate change and the challenges in the Union's Eastern Neighbourhood. The Strategy reflects a *paradigm shift*: the Black Sea is no longer treated as a fringe of Europe, but as a space essential for the future security and prosperity of the European Union.

In terms of content, the approach is organized around *three main pillars*: security, stability, resilience; sustainable growth and prosperity; and environmental protection, climate change adaptation and civil protection. The Strategy includes several key projects that unite the three pillars: a regional hub for maritime security in the Black Sea; an energy, transport and digital connectivity agenda; and other actions to support partners in the region (Ukraine, the Republic of Moldova, Georgia, Armenia, Azerbaijan, Turkey) to benefit from cooperation with EU policies.

The first pillar focuses on strengthening maritime security and regional resilience. The strategy proposes the creation of a regional maritime security hub, focused on maritime intelligence collection and analysis, civil-military cooperation in the field of maritime security, monitoring of critical offshore infrastructure and data sharing between national institutions, the EU and regional partners. This would eventually become the core of regional cooperation between EU Member States and coastal partners. In addition, the importance of intensifying cooperation in the field of maritime mine clearance – which already benefits, starting from 2024, from a unified approach of the Black Sea littoral states through the establishment of the *MCM Black Sea Task Force* (Semnarea Memorandumului de Înțelegere privind constituirea grupului operativ pentru combaterea minelor marine în Marea Neagră/ Memorandum of Understanding on the establishment of the Task Force to Counter Sea Mines in the Black Sea – Mine Countermeasures Black Sea/MCM Black Sea, 2024), countering hybrid and cyber threats, as well as the security of submarine energy infrastructures are highlighted. At the same time, emphasis is placed on the interoperability of naval forces and on strengthening rapid response capabilities in the event of a crisis.

The strategy introduces, through the second pillar, a dedicated connectivity agenda, focused on transport (through the corridors related to the Trans-European Transport Network – TEN-T²), energy and digitalization, which aims to extend European corridors to Central Asia through the Caucasus. By modernizing transport corridors and developing energy interconnections, the EU aims to reduce dependence on traditional routes controlled by unstable actors and create an integrated economic space on the Black Sea, competitive and resilient.

The third pillar reflects the concern for sustainability and environmental risk management. The strategy proposes common mechanisms for preparing for and responding to natural or man-made disasters, combating pollution and coastal erosion, and protecting marine ecosystems. At the same time, the document supports the development of green offshore energy, in particular wind projects, and encourages the protection of submarine infrastructure, essential for communications and energy transport. The ecological approach of the strategy is complementary to the security objectives, as environmental degradation and climate change can generate new strategic vulnerabilities.

ROMANIA – CHALLENGES AND OPPORTUNITIES

Romania is one of the states onto which the developments and risks in the region have a direct impact, so the EU's strategic approach for the Black Sea region can create opportunities. Thus, the first of them is the *consolidation of the geostrategic role*. Romania can become a regional hub for maritime security, by actively participating in its structure and by cooperating with the other littoral states. A first step in this direction has already been taken at the ministerial meeting³ on trans-regional security and connectivity, organized on the margins of the Foreign Affairs Council on 20 October 2025, by presenting Romania's availability to host the hub on maritime security. Beyond the obvious benefit from a security perspective, other advantages that such a proactive approach would create would be increasing the capacity to react to hybrid threats and sabotage on offshore infrastructure, creating specialized jobs in security, IT and marine analysis, as well as positioning Romania as a regional hub for EU – NATO – Eastern partners cooperation.

² *Trans-European Transport Network (TEN-T): The Council gives final green light to new regulation ensuring better and sustainable connectivity in Europe*, press release, European Council, 13 June 2024, <https://www.consilium.europa.eu/ro/press/press-releases/2024/06/13/trans-european-transport-network-ten-t-council-gives-final-green-light-to-new-regulation-ensuring-better-and-sustainable-connectivity-in-europe/>, retrieved on 24 September 2025.

³ *Participation of the Minister of Foreign Affairs, Oana Țoiu, in the Ministerial Meeting on Security and Trans-Regional Connectivity, organized on the margins of the Foreign Affairs Council*, MFA press release, 20 October 2025, <https://mae.ro/node/67627>, retrieved on 21 October 2025.

In relation to the proposals in the document, Romania can also increase its role in military and logistical mobility, through adapted port and transport infrastructure (airports, railways etc.). A second benefit lies in *improvements in security and resilience*, by ensuring the protection of critical infrastructure, as well as through increased cooperation in preventing hybrid and disinformation threats.

Romania can also capitalize on European investments for the modernization of port and railway infrastructure, contributing to the military and logistical mobility of the Union. The benefits are, however, conditional on the absorption capacity of European funds, efficient inter-institutional coordination and the maintenance of a sustained political commitment. Thus, planned investments in port, railway and airport infrastructure must be designed with a dual purpose: supporting civil mobility and increasing the Union's military and logistical mobility capacity.

Among the challenges that Romania could face are: limitations in administrative and financial resources; persistent risks generated by the conflict in Ukraine; as well as the complexity of multilateral cooperation with diverse partners, sometimes with divergent interests.

First, although the tendency is to focus on the security perspective, namely on the creation and operationalization of the regional maritime security hub, the *implementation of the EU strategic approach to the Black Sea* should be viewed in its entirety. This means, on the one hand, approaching the other two pillars of the strategy with similar attention and, on the other hand, close coordination and, possibly, institutionalized through an inter-ministerial group-type mechanism, with the participation of institutions with responsibilities in the field, but also the creation of a fund dedicated exclusively to the Black Sea region. Fragmented management of lines of effort can be effective only in the respective segment, and in this case, a unitary approach can be the key to the successful implementation of the EU strategic approach in its entirety.

The EU strategic approach to the Black Sea is an important step, providing a coherent framework for action in the area of security, development and environment. For Romania, it means an opportunity to strengthen its regional role, attract investment and enhance national security, but its success will depend on its properly reflecting the lines of effort into concrete policies and projects. The lack of a clear financial mechanism, fragmentation of institutional competences and poor coordination with other partners may affect implementation.

CONCLUSIONS

The *European Union's Strategic Approach to the Black Sea Region* signifies a maturity reach of European security policy and a reaffirmation of the commitment to the stability of the Eastern flank. The Black Sea can represent not only a risk

perimeter, but also a vector of European integration and projection of stability towards the eastern neighbourhood.

Beyond the national framework, it is essential to emphasize that the responsibility for implementing the strategy belongs to all EU Member States. Furthermore, it is useful to see the strategy as a piece in a puzzle, with the document also highlighting synergies with other EU policy frameworks and initiatives, such as the Eastern Partnership, the EU Strategic Compass for Security and Defence, the revised EU Maritime Security Strategy and the Global Gateway, the Common Maritime Agenda for the Black Sea, as well as the Common Strategic Agenda for Research and Innovation for the Black Sea. In addition, implementation efforts need to be reflected in EU-NATO cooperation, both at the political level (e.g. by renewing the Joint Declaration on cooperation between the two, the most recent of which dates back to 2023) and at the practical level, by identifying the complementarity of existing measures and initiatives and making the best use of them. In addition, cooperation with Türkiye, including from the perspective of guardian of the 1936 Montreux Convention (1936 Convention regarding the Regime of the Straits, 1936), will be another element that will determine the efficiency and sustainability of the EU Strategic Approach to the Black Sea.

For Romania, this document does not represent just a political framework, but a strategic opportunity to assert itself as a key regional actor – through active participation in security, development and environmental initiatives, in an *inter-institutional synergy*. Capitalizing on this position will depend on the capacity to articulate coherent policies, to cooperate effectively at regional level with the Black Sea littoral states and at European level with the other EU Member States, as well as to integrate the security dimension with that of sustainable development.

BIBLIOGRAPHY:

1. Baylis, J., Wirtz, J.J., Colin, G.S. (2016). *Strategy in the Contemporary World: An Introduction to Strategic Studies*. Oxford: Oxford University Press.
2. *Black Sea Synergy – A New Regional Cooperation Initiative* (4 November 2007), Brussels, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52007DC0160&from=EN>, retrieved on 20 September 2025.
3. *Black Sea Synergy: 4th review of a regional cooperation initiative – period 2019-2023* (3 July 2024), Brussels, <https://data.consilium.europa.eu/doc/document/ST-11900-2024-INIT/en/pdf>, retrieved on 24 September 2025.
4. *Black Sea Strategic Research and Innovation Agenda* (10 June 2019). Bucharest, https://www.mae.ro/sites/default/files/file/anul_2019/2019_pdf/black_sea_strategic_research_and_innovation_agenda.pdf, retrieved on 22 August 2025.
5. Coffey, L., Kasapoğlu, C. (February 2023). *A New Black Sea Strategy for a New Black Sea Reality*. Hudson Institute, <http://media.hudson.org.s3.amazonaws.com/A+New+Black+Sea+Strategy+for+a+New+Black+Sea+Reality.pdf>, retrieved on 22 August 2025.

6. *European Council Conclusions, 23-24 June 2022* (24 June 2022), Brussels, <https://www.consilium.europa.eu/media/57442/2022-06-2324-euco-conclusions-en.pdf>, retrieved on 20 September 2025.
7. *Joint Communication to the European Parliament and the Council, the European Union's Strategic Approach to the Black Sea Region* (28 May 2025), Brussels, https://enlargement.ec.europa.eu/document/download/170d9b3a-d45f-4169-80fa-9adb753c0921_en?filename=EU%20Strategic%20Approach%20Black%20Sea%20Strategy.pdf, retrieved on 21 August 2025.
8. Kakachia, K., Malerius, S., Meister, S. (ed.) (2024). *Security Dynamics in the Black Sea Region: Geopolitical Shifts and Regional Orders*. Springer.
9. MAPN (14 September 2025). *Fragmente de drone folosite de Rusia în războiul din Ucraina, identificate pe teritoriul României*, Agerpres, București, <https://agerpres.ro/social/2025/09/14/mapn-fragmente-de-drone-folosite-de-rusia-in-razboiul-din-ucraina-identificate-pe-teritoriul-romaniei--1484106>, retrieved on 20 September 2025.
10. McCabe, R., Sanders, D., Speller, I. (2020). *Europe* (ed.). *Small Navies and Maritime Security. Balancing Traditional Roles and Emergent Threats in the 21st Century*. New York: Routledge.
11. *Ministerial Declaration on a Common Maritime Agenda for the Black Sea* (19 May 2019), Bucharest, https://www.mae.ro/sites/default/files/file/anul_2019/2019_pdf/0514_ministerial_declaration_on_the_common_maritime_agenda_for_the_black_sea_-_final.pdf, retrieved on 24 September 2025.
12. *Participation of the Minister of Foreign Affairs, Oana Tîoiu, in the Ministerial Meeting on Security and Trans-Regional Connectivity, organized on the margins of the Foreign Affairs Council*, MFA press release (20 October 2025), <https://mae.ro/node/67627>, retrieved on 21 October 2025.
13. *Trans-European Transport Network (TEN-T): The Council gives final green light to new regulation ensuring better and sustainable connectivity in Europe*, press release, European Council (13 June 2024), <https://www.consilium.europa.eu/ro/press/press-releases/2024/06/13/trans-european-transport-network-ten-t-council-gives-final-green-light-to-new-regulation-ensuring-better-and-sustainable-connectivity-in-europe/>, retrieved on 24 September 2025.
14. *Semnarea Memorandumului de Înțelegere privind constituirea grupului operativ pentru combaterea minelor marine în Marea Neagră/The Memorandum of Understanding on the establishment of the Task Force to Counter Sea Mines in the Black Sea – Mine Countermeasures Black Sea/MCM Black Sea*, press release, Bucharest (11 January 2024), https://www.mapn.ro/cpresa/18251_semnarea-memorandumului-de-intelegere-privind-constituirea-grupului-operativ-pentru-combaterea-minelor-marine-in-marea-neagra, retrieved on 24 September 2025.
15. *Black Sea Strategy: Press remarks by the High Representative of the Union for Foreign Affairs and Security Policy/Vice-President of the European Commission, Kaja Kallas* (28 May 2025), https://www.eeas.europa.eu/eeas/black-sea-strategy-press-remarks-high-representativevice-president-kaja-kallas_en, retrieved on 10 September 2025.
16. *1936 – Convention regarding the Regime of the Straits* (20 July 1936), Switzerland: Montreux, <https://cil.nus.edu.sg/wp-content/uploads/2019/02/1936-Convention-Regarding-the-Regime-of-the-Straits-1.pdf>, retrieved on 21 August 2025.

INFORMATION INTELLIGENCE SYSTEMS AND MACHINE-LEARNING ALGORITHMS FOR ADAPTIVE DECISION-MAKING IN THE EASTERN SECURITY LANDSCAPE

Associate Professor Dr. Florentina-Loredana DRAGOMIR

"Carol I" National Defence University, Bucharest

DOI: 10.55535/RMT.2025.3.15

The study investigates the role of intelligence-type information systems integrated with machine-learning algorithms in supporting adaptive decision-making within Eastern security, in the context of regional crisis scenarios. The research aims to develop a predictive model capable of anticipating the potential distribution of Moldovan refugees across European states, using a set of variables relevant to the dynamics of forced migration: distance from the Republic of Moldova, cultural similarities, religious similarities, living standards, and the historical number of refugees. The methodology is based on the use of the RandomTree algorithm from the WEKA platform, selected for its ability to generate interpretable models and its suitability for multicriteria classification problems in the field of security.

The resulting decision tree highlights distance as the primary factor shaping initial mobility, followed by cultural and religious determinants for neighbouring states, and economic and diasporic indicators for more distant destinations. The hierarchical structure of the tree confirms the hypothesis that relocation decisions are the result of a complex interaction between geographical proximity, socio-identity affinities, and socioeconomic attractiveness.

Integrating this analysis into intelligence information systems enhances the capacity of security institutions to anticipate mobility flows in crisis situations, providing a robust and transparent predictive tool useful for resource planning, early warning, and developing adaptive strategies in the Eastern neighbourhood.

Keywords: information system; intelligence; machine learning; adaptive decision-making; WEKA platform;

INTRODUCTION

The transformations within the geopolitical landscape of Eastern Europe, amplified by military aggression, internal instability, and hybrid pressures, require a new operational framework for risk management and decision-making in the field of security. In this regard, intelligence-type information systems become essential for the real-time assessment of crisis dynamics, particularly with respect to forced migration and population mobility (Dragomir, 2023-a, 2025).

For example, in the case of the Republic of Moldova – strategically positioned between Eastern and Western spheres of influence – a regional crisis may generate significant refugee flows. Anticipating such phenomena requires integrating predictive models into the state’s informational architecture (Dragomir, Enache, 2023). The use of machine-learning (ML) algorithms, such as RandomTree, facilitates not only the analysis and classification of possible scenarios but also the clear interpretation of the main determinants of mobility: geographical distance, cultural affinities, economic factors, and the presence of a historical diaspora (Azizyan, Gheisari, 2025; Dragomir, 2021-b).

This approach aligns with the paradigm of algorithmically assisted adaptive decision-making, which brings to the forefront the idea of a proactive institutional response supported by multi-level information systems (Dragomir, 2023-b). Thus, the multi-layered analysis of data – ranging from digital monitoring of radicalization trends to ideological modelling of terrorism – becomes an integrated component of security policy (Dragomir, 2025-c; Dragomir, Alexandrescu, Postolache, 2018).

At the same time, the ethical dimension of using such systems cannot be neglected. The “*confidentiality – loyalty – responsibility*” triad provides an indispensable normative framework within modern decision-making architectures (Dragomir, 2021-e). Moreover, algorithmic transparency becomes a legal necessity in the context of protecting fundamental rights, being closely linked to the legality of automated decisions (Dragomir, 2022-d).

Therefore, in regional crisis scenarios such as the one analysed in this study, the combined use of information systems and ML-assisted predictive models ensures a superior institutional response capacity. This capacity is essential for strategic planning, resource allocation, and maintaining stability in the Eastern neighbourhood (Pietras, 2025; Thomas, 2024).

INTELLIGENCE INFORMATION SYSTEMS SUPPORTING ADAPTIVE DECISION-MAKING

The ability of a military organization or state to anticipate, interpret, and rapidly respond to changes in the operational environment depends decisively on the quality of its informational infrastructure and on the level of integration between data, analysis, and algorithms. Adaptive decision-making relies on a continuous flow of relevant information, processed in real time and contextualized through advanced analytical methods. In this regard, intelligence information systems become integrated platforms that connect various types of data – structured, semi-structured, or unstructured – with predictive models capable of supporting strategic and operational actions in a volatile environment.

❖ **Data Collection (Data Acquisition Layer)**

The first layer integrates all relevant information sources needed to build a comprehensive situational picture. This stage includes ISR systems (electro-optical, radar, satellites), OSINT sources – originating from social networks, media streams, or public databases – HUMINT components such as field reports and direct observations, to which SIGINT and CYBINT flows may be added in specialized contexts.

The diversity of these data types, ranging from images and raw signals to structured or unstructured text content, requires advanced protocols for integration, filtering, and validation, designed to reduce uncertainty and enhance the reliability of subsequent decisions. Additionally, the system must incorporate automatic anomaly-detection mechanisms that identify deviations from typical patterns and filter out irrelevant or compromised information.

❖ **Data Processing and Storage (Data Processing & Storage Layer)**

During the processing stage, collected data undergo automated cleaning, transformation, and semantic labelling to ensure compatibility with analytical models in the upper layers. This type of processing is followed by storage in a secure infrastructure, which may include relational databases, data lakes, or hybrid platforms optimized for scalability and distributed access. Managing massive volumes of mission-critical data requires implementing advanced cybersecurity standards and strict access-control policies to safeguard the integrity and confidentiality of the information.

❖ **Algorithm-Assisted Analysis (Analytics & ML Layer)**

This analytical level represents the space where the strategic value of the information system is fully realized, as traditional cognitive processes of analysts are augmented by advanced algorithmic tools. They include classification and regression

techniques, pattern-detection methods, clustering and similarity analysis, predictive models such as decision trees, neural networks, or Bayesian structures, as well as adaptive learning systems capable of updating parameters in real time.

Integrating machine learning into this layer not only optimizes information processing but also enables forecasting of potential developments, generating alternative scenarios, early detection of emerging threats, and significant reduction of cognitive biases inherent in exclusively human analysis.

❖ **Dissemination and Decision Support (Decision Support Layer)**

The final layer of the architecture focuses on delivering analytical results to decision-makers in a clear, accessible, and operational format. It is achieved through intuitive graphical interfaces, interactive dashboards, automated alerting systems, and advanced data-visualization tools.

The core purpose of this layer is to reduce the time between the occurrence of an event and the strategic response, thereby enabling adaptive, robust, and context-aware decisions. Essentially, this level transforms processed information into actionable knowledge capable of supporting planning, risk assessment, and real-time operational coordination.

Recent research highlights a significant shift in the development paradigm of intelligence information systems, which are moving from static architectures toward dynamic, adaptive designs capable of functioning under conditions of disrupted and volatile operational environments. These systems are designed not only to collect and analyse data but also to learn and react in real time to emerging threats or informational disruptions, particularly in complex military theatres (Wang et al., 2025; Smaliukienė, Giedraitytė, 2025).

A reference example in this direction is represented by new-generation anti-jamming systems used in active conflict zones, where maintaining uninterrupted communication becomes critical for ensuring operational advantage. The architecture proposed by Wang et al. (2025) introduces an advanced multidimensional transfer-learning model that enables automatic recognition of modifications in the electromagnetic spectrum – typically caused by enemy electronic interference – and adjustment of transmission protocols to ensure continuity and security of transmitted data.

This approach provides two essential tactical advantages:

❖ **Real-time adaptivity** – The system relies on advanced reinforcement-learning and online-learning techniques, continuously adjusting its parameters according to changes in the electromagnetic environment. Practically, the system becomes

“intelligent” in the sense that it evolves alongside the operational context without constant human intervention (Wang et al., 2025).

❖ **Resilience to infrastructure degradation** – In environments characterized by instability, physical destruction, or severe radio interference, the architecture maintains critical communication functionality through self-optimization and distributed redundancy, as demonstrated by tactical simulations and stress tests (Ib.).

Furthermore, this research direction aligns with the broader trend of developing cognitive information systems – systems that not only “respond” to stimuli but “understand” the operational context by integrating multisource data and generating highly reliable predictions even under conditions of systemic uncertainty (Byranvand, 2025; Smaliukienė, Giedraitytė, 2025). This aspect fundamentally transforms real-time decision-making, offering a significant strategic advantage in hybrid conflict and electronic warfare environments.

The adaptive decision-making approach in the context of modern security and information management presupposes the use of machine-learning (ML) algorithms as analytical and operational support tools. These technologies are especially applied in two main directions, essential for the efficiency of real-time decision-making and for reducing uncertainty.

Algorithms such as *RandomTree* or reinforcement learning are already implemented in areas such as refugee-distribution analysis, environmental monitoring, or autonomous network surveillance. In these cases, the generated models are explainable, rule-based, and allow decision-makers to quickly understand the logical structure behind predictions (Kumar, Shekhar, Tewary, 2025). For example, Dwivedi (2025) proposes an analytical framework for intelligent energy systems, based on partially observable decision-process modelling (POMDP), which enables continuous updating of predictions based on real-time data. This approach offers critical flexibility in dynamic contexts such as those generated by humanitarian crises or unpredictable military actions.

Another major benefit of using ML is its ability to reduce uncertainty within large datasets, often ambiguous or incomplete. ML technologies contribute to clarifying the Common Operational Picture (COP) by eliminating informational noise and extracting the most relevant variables (Kothinti, 2025). ML systems implemented in adaptive architectures – such as those in the automotive or military domains – significantly improve decision coherence and strategic agility by rapidly identifying anomalies, updating risk scenarios, and suggesting actions based on learning from historical and contextual data (Park, 2025; Thomas, 2024).

METHODOLOGY

❖ Conceptual Foundation of the Model

The methodology used in this study is based on the application of the RandomTree algorithm, available in the WEKA platform, for analysing and modelling the potential distribution of Moldovan refugees under regional crisis scenarios. The choice of RandomTree was grounded in the need for a method capable of generating an explicitly interpretable model that highlights the relationships among the key variables underlying forced mobility. RandomTree is a non-ensemble algorithm that constructs a single decision tree. Unlike Random Forest, it does not aggregate the results of multiple trees; instead, it generates a unique structure whose branches are influenced by the random selection of attribute subsets. This characteristic makes it a valuable exploratory instrument, enabling the identification of variables with high predictive power in the spatial distribution of refugees.

❖ Fundamental Parameters of the Model

The RandomTree model was built using four variables considered essential for explaining a refugee’s decision under conditions of uncertainty. The parameters were selected based on specialized literature on forced migration and on the availability of comparable data.

❖ Geographical Distance from the Republic of Moldova

The physical distance between the analysed states and the Republic of Moldova constitutes a fundamental logistical indicator with a decisive role in shaping the initial flows of human mobility. Within the context of decision modelling, this variable emerges as the root of the classification tree, confirming its strategic importance in anticipating the behaviour of populations under critical pressure.

Territorial proximity influences not only the speed at which a population may access the territory of a neighbouring state, but also that state’s institutional capacity to manage an immediate influx – reducing transit costs, travel risks, and logistical barriers. Thus, geographical distance becomes the first filter structuring migration scenarios, functioning as a structural determinant of accessibility and reaction time for both individuals and state response mechanisms.

(A) Bulgaria (B) Croația (C) Germania (D) Italia (E) Polonia (F) România (G) Rusia (H) Serbia (I) Spania (J) Suedia (K) Ucraina											
Indicatori	TARI										
	A	B	C	D	E	F	G	H	I	J	K
Distanța (Km)	820	1541	1519	2291	968	435	1344	946	3584	2594	487

Table 1: Geographical distance (in kilometres) between the Republic of Moldova and the analysed states
(author’s design)

❖ **Cultural Similarities**

This aggregated indicator reflects the degree of identity proximity between the population of the Republic of Moldova and communities in the potential destination states, integrating elements related to language, traditions, shared historical references, and normative compatibility. In the analytical model, cultural similarities significantly influence relocation preferences, especially within immediate geographical spaces where the cultural barrier is minimal and the probability of rapid integration is considerably higher.

From this perspective, the variable functions as a facilitator of mobility, reducing perceived uncertainty, lowering the costs of social adaptation, and strengthening the sense of familiarity between origin and destination communities. The algorithm used this parameter to model the spontaneous choices of refugees, suggesting that, in the absence of other major constraints, cultural proximity can become a determining factor in the initial direction of migration.

❖ **Religious Similarities**

The variable referring to confessional compatibility captures the value-oriented dimension of the migration process, having direct implications for the potential of social integration within host communities. In states where the religious structure is similar to that of the Moldovan population, the climate of acceptance and community cohesion can consolidate more rapidly, reducing sociocultural tensions and facilitating individuals' participation in social and civic life.

In modelling relocation behaviour, religious similarities function as an indicator of normative and symbolic compatibility, influencing refugees' willingness to choose states in which spiritual values and religious practices do not constitute a barrier but rather an element of identity continuity.

❖ **Standard of Living in the Analysed States**

This socioeconomic parameter – articulated through indicators such as GDP per capita, cost of living, and purchasing power – represents one of the most important factors shaping destinations located at medium and long distances.

Unlike variables associated with geographical or cultural proximity, the standard of living acts as an attractor in the later phases of mobility, when individuals begin to prioritize economic opportunities, financial stability, and long-term prospects.

The algorithm integrated this indicator as a decisive node in the tree structure, signalling that states with a high level of prosperity tend to be perceived as preferred final destinations, even if the distance implies a higher migration cost. Therefore, the standard of living becomes a relocation-optimization factor, guiding populations toward spaces offering the best prospects for sustainable economic integration.

Indicatori	ȚĂRI										
	A	B	C	D	E	F	G	H	I	J	K
Nivel de trai pe cap de locuitor	29177	37549	63834	51061	42465	38096	31967	23534	46551	63877	14150
Procent comparativ cu cel din R. Moldova (16482)	1.77	2.28	3.87	3.10	2.58	2.31	1.94	1.43	2.82	3.88	0.86

Table 2: Standard of living in the Republic of Moldova and the analysed states (author’s design)

❖ Dataset Construction

The dataset used in this study was constructed by operationalizing the four selected parameters into discrete values corresponding to ordered classes, allowing the model to capture significant differences between states without depending on numerical variations that are difficult to compare. The dataset development process included a systematic stage of normalizing and standardizing distance intervals to ensure the geographical relevance of each state in relation to the Republic of Moldova. In parallel, socioeconomic values such as GDP per capita, cost of living, and other indicators of living standards were classified into comparative ranks, enabling their transformation into a format usable by the RandomTree algorithm without losing conceptual significance. Regarding the socio-identity dimension, cultural and religious variables were aggregated into ordered categories based on their degree of similarity to the Republic of Moldova – an approach that contributed to shaping interpretable causal relationships within the decision tree. Additionally, data on the Moldovan diaspora were incorporated through the inclusion of values related to the relative number and distribution of pre-existing Moldovan refugees in the analysed states, an indicator integrated to capture network effects that significantly influence migratory behaviour. This stratified and coherent structuring of data allowed the RandomTree algorithm to generate clear, consistent, and easily interpretable branches, maximizing the analytical utility of the model.

RESULTS

The RandomTree algorithm was configured using the default settings of the WEKA platform, as they provide an optimal balance between exploring data structure and preventing overfitting. The configuration included the random selection of attribute subsets during the construction of each node – a mechanism that introduces controlled variability and allows the identification of combinations of factors with high predictive power. To maintain an adequate degree of generalization and avoid excessive model complexity, tree-depth limitation was applied, preventing the

generation of overly detailed branches that would not significantly contribute to interpretability or accuracy. Model robustness was evaluated using a cross-validation procedure, which enabled performance testing across multiple dataset partitions and reduced the influence of potential statistical peculiarities of the sample. Unlike ensemble models, RandomTree generated a single decision tree, allowing for direct interpretation of the resulting causal chain. The final model presents an extended tree whose nodes are logically organized according to information gain and controlled random selection process, offering a coherent picture of how each parameter contributes to the probable distribution of refugees in the analysed scenario.

Applying the RandomTree algorithm to the dataset constructed from the four selected parameters generated an extensive decision tree in which *geographical distance from the Republic of Moldova* emerged as the root variable, confirming its role as the primary determinant of refugee mobility during crises. The model shows that when distance is minimal, relocation behaviour is predominantly influenced by cultural similarities, indicating that states such as Bulgaria, Ukraine, and Romania are preferred depending on the degree of identity proximity, which underscores the importance of socio-historical continuities in the early phases of forced migratory flows. As distance increases, the decision tree shifts from identity-based criteria to confessional compatibility: at moderate distances, religious similarities become the major discriminating factor, directing flows toward states such as Poland, Serbia, or again Bulgaria, depending on doctrinal concordances and familiar community structures. For greater distances, economic factors become decisive: the standard of living in the analysed states gains significant relevance, and the algorithm identifies a distribution oriented toward destinations such as Croatia, Russia, or Germany – states perceived as possessing superior socioeconomic absorption capacity and medium-term stabilization potential. Finally, for the most distant destinations, the tree structure reveals a heightened role of the historical presence of Moldovan refugees, suggesting that diaspora-driven network effects function as a dominant attractor.

This dynamic is visible in the model's orientation toward states such as Sweden, Spain, or Italy, where established Moldovan communities reduce the psychosocial costs of transition and facilitate informal support and integration mechanisms. Overall, the results provided by the RandomTree model reveal a stratified decision structure in which geographical proximity acts as the primary selection factor, followed by cultural and religious identity at short and medium distances, and, at greater distances, by economic factors and diaspora distribution.

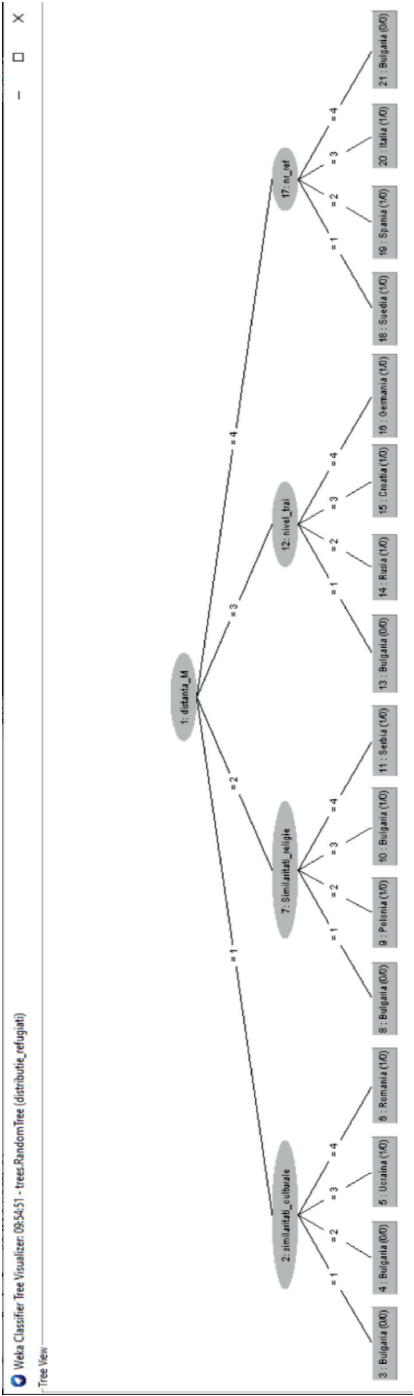


Figure 1: Random Tree Decision Tree (author’s design)

This pattern indicates the existence of a complex, multilevel logic governing migratory behaviour during regional crisis scenarios.

DISCUSSION

The analysis of the results obtained through the RandomTree algorithm highlights a deeply stratified decision architecture in which each parameter contributes differently to modelling the relocation behaviour of Moldovan refugees under conditions of regional crisis. The dominance of distance as the primary factor confirms, first and foremost, the fundamental thesis in the literature on forced mobility, which states that geographical proximity represents the immediate criterion of any initial displacement. Individual decision-making is strongly anchored in the need for speed, safety, and reduced exposure to risk, which explains the immediate orientation toward states in direct territorial proximity. The role of cultural and religious similarities, evident in the branches corresponding to short and medium distances, underlines the decisive influence of collective identity on migratory behaviour. Choosing states perceived as culturally or confessionally close suggests the existence of a logic of familiarity-seeking, in which refugees prefer environments that reproduce – at least partially – the sociocultural patterns of their place of origin. This orientation aligns with theories of social capital and recent studies on integration within host communities, which show that identity similarities simplify transition, reduce psychological stress, and provide an immediate sense of continuity.

As distance increases, the model indicates a transition from identity-related factors to structural factors, particularly economic ones. The emergence of the standard of living as a decisive variable for long-distance destinations suggests that, in the absence of cultural familiarity, refugees become far more sensitive to the availability of material opportunities. This logic indicates a strategic behaviour oriented toward financial stability, access to services, and institutional protection – elements capable of compensating for the disadvantages of greater distance and sociocultural differences.

For the most distant destinations, RandomTree reveals the strong importance of the historical number of Moldovan refugees, indicating the robustness of network effects. The presence of an established diaspora in states such as Italy, Spain, and Sweden not only signals the availability of potential community support but also acts as a mechanism for reducing uncertainty through access to information, logistical assistance, and already validated adaptation strategies. This finding aligns consistently with migration network theories and highlights an important empirical

reality: migration flows tend to become self-reinforcing over time, consolidating through transnational connections. Taken together, the discussions derived from the RandomTree model confirm that relocation decisions in crisis situations cannot be reduced to a single factor, but instead represent the expression of an adaptive interaction between proximity, identity, and economic structure. This multidimensional perspective is essential for designing security and migration-management policies that are sensitive to the real dynamics of human behaviour and can provide precise instruments for strategic anticipation in the Eastern security context.

CONCLUSIONS

The analysis conducted using the RandomTree algorithm highlights a complex and stratified decision architecture, deeply dependent on the interaction between geographical proximity, identity compatibilities, and socioeconomic attractiveness – elements that decisively shape the behaviour of Moldovan refugees in regional crisis scenarios. The results allow the formulation of major conclusions regarding the dynamics of forced mobility and the usefulness of machine-learning-based modelling in the context of Eastern security. The emergence of geographical distance as the root variable confirms that human mobility under conditions of instability is governed, in its initial phases, by pragmatic criteria related to the urgency of crossing safer spaces with minimal exposure to operational risks. This finding validates the specialized literature and supports the integration of distance as a strategic indicator in information systems used for anticipating migratory flows.

The relevance of cultural and religious similarities in relocation choices associated with short and medium distances reflects the fact that identity proximity remains an essential determinant of relocation, significantly influencing perceptions of social continuity and psychological safety. Remarkably, the model shows that refugees do not orient themselves exclusively toward the closest states, but rather toward those that offer a familiar cultural or confessional environment. It suggests the necessity of a multidisciplinary approach to understanding forced migration.

The emergence of the standard of living as a dominant variable for distant destinations confirms that refugees' decisions evolve from immediate reactions to medium-term adaptive strategies, in which economic, institutional, and welfare-related criteria become priorities. This transition highlights that mobility during crises is not a one-dimensional phenomenon, but one characterized by a progressive evolution of motivations. The strong role of the network effect, reflected through

the historical number of Moldovan refugees, demonstrates that the diaspora functions as a central vector in shaping flows toward distant states, constituting an informal resource that reduces uncertainty, facilitates integration, and influences long-term patterns of mobility. This conclusion is especially relevant for public policy, indicating the need to monitor the evolution of diasporic communities as an instrument for anticipating migratory pressures.

Overall, the study demonstrates that the use of ML algorithms such as RandomTree within intelligence-type information systems can significantly strengthen early-warning capabilities, strategic planning, and adaptive management of population flows in the context of Eastern security. At the same time, the research highlights both the potential and the current limitations of data-assisted modelling, suggesting future directions for development that include expanding datasets, integrating dynamic geopolitical indicators, and developing hybrid machine-learning architectures capable of capturing the evolving complexity of the operational environment. The results obtained through modelling the migratory behaviour of Moldovan refugees have significant strategic implications for regional security architecture, as they describe with a high degree of granularity the mechanisms through which potential population flows may be redirected during crises, revealing critical elements that can support proactive public policies.

BIBLIOGRAPHICAL REFERENCES:

1. Azizyan, O., Gheisari, M. (2025). *Security Strategy for West Asia Water Crisis. Iranian Review of Foreign Affairs.*
2. Byranvand, F.N. (2025). *Buck-passing System as a Security Order in East Asia: Requirements and Contexts for US Action.* International Relations Studies.
3. Dragomir, F.-L. (2025-a). *Algorithmic Transparency in Information Systems: A Legal Necessity for the Protection of Fundamental Rights.* Acta Universitatis Danubius. Juridica, 21(1), pp. 126-136.
4. Dragomir, F.-L. (2025-b). *How information systems are reshaping national security strategies*, in *Romanian Military Thinking*, no. 1, pp. 202-213. Defence Staff.
5. Dragomir, F.-L. (2025-c). *Integrating artificial intelligence into operational research – New horizons for national security*, in *Romanian Military Thinking*, no. 1, pp. 174-187. Defence Staff.
6. Dragomir, F.-L., Enache, R. (2025). *Information Systems in the Analysis of Ideological Terrorism Modeling: the Interaction between Attacks, Arrests and Convictions in Europe (2017-2022)*, in *Romanian Military Thinking*, no. 2. Defence Staff.
7. Dragomir, F.-L., Alexandrescu, G., Postolache, F. (2018). *Tools for Hierarchical Security Modeling.* The 14th International Scientific Conference eLearning & Software for Education, Bucharest: "Carol I" National Defence University, 4(10.12753/2066-026X-18-219), pp. 34-38.

8. Dragomir, F.-L. (2025-e). *Multilevel architecture of information systems for monitoring radicalization trends in digital environments*, in *Romanian Military Thinking*, no. 1. Defence Staff.
9. Dragomir, F. (2017). *Aspects of the information security model*. "Securitate Națională, Europeană și Euroatlantică" Scientific Communication Session, 3, pp. 184-190.
10. Dragomir, F.-L. (2024). *The potential for intensifying Austria's opposition to Schengen enlargement*, in *European Journal of Accounting, Finance & Business*, 12(2), pp. 120-128. ISSN 2344-102X, no. 2/June 2024 ISSN-L 2344-102X DOI: 10.4316/EJAFB.2024.
11. Dragomir, F.-L. (2025-f). *Confidentiality, Loyalty, and Responsibility: The Ethical Triad in Information Systems Management in the Field of National Security*, in *Bulletin of "Carol I" National Defence University*, 14(2), pp. 296-310;
12. Dragomir-Constantin, F.-L., Beldiman, C.M., Zlati, M.L. (2025). *Informational Approaches in Modelling Social and Economic Relations: Study on Migration and Access to Services in the European Union*. Systems, 13(6), 469. MDPI.
13. Dragomir-Constantin, F.-L. (2025-d). *Modeling Fiscal Pressure for Economic Resilience: An Intelligent Information System Approach Based on J48 Tree*. Acta Universitatis Danubius. Economica, 21(3). University Danubius Press.
14. Dwivedi, A. (2025). *Power system analytics: anomaly detection, prediction, and mitigation*. Rensselaer Polytechnic Institute.
15. El Ghamari, M. (2025). *Strategic Thinking: Geopolitical Rivalry in the Middle East*. Wojsko Polskie.
16. Ismail, H., Muñoz González, I.G. (2025). *The Geopolitics of Central Bank Digital Currencies*. EUI Working Papers.
17. Kothinti, G.R. (2025). *Machine Learning-Enhanced Scalable Architectures for Safe and Connected Autonomous Vehicles*, in *International Journal of Humanities and Information Technology*, 11(2).
18. Kumar, D., Shekhar, S., Tewary, T. (2025). *AI and data analytics for climate data management*. Frontiers in Environmental Science, 13, Article 1679608.
19. Murphy, G. (2025). *Security Ecosystems and Decentralized Intelligence in Europe*. NATO Review.
20. Özer, C. (2025). *Territorial Waters Dispute in the Aegean Sea and its Strategic Consequences*. Kent University.
21. Park, D. (2025). *Data-driven trajectory prediction for reliable autonomous driving systems*. KAIST.
22. Pietras, M. (2025). *The crisis of international arms control regimes and the new phase of geopolitical rivalry*. International Relations Publishing.
23. Smaliukienė, R., Giedraitytė, V. (2025). *The Migration Crisis Artificially Created by the Belarusian Regime: A Case Study of Military Engagement in Lithuania*. In *Democratic Resilience in the Baltics*, vol. 1. Springer.
24. Thomas, P. (2024). *Integrating Reservoir Simulation and Real-Time Data Analytics for Enhanced Field Optimizer Performance in Thermal EOR Operations*. ResearchGate.
25. Wang, S., Wang, X., Ke, Z., Liu, D., Liu, J., & Du, Z. (2025). *Multi-Mode Anti-Jamming for UAV Communications: A Cooperative Mode-Based Decision-Making Approach via Two-Dimensional Transfer Reinforcement Learning*, in *Journal of Electronics & Information Technology*.

REDEFINING DETERRENCE: WARFARE IN THE TECHNOLOGICAL ERA

Colonel Dr. Tiberius TOMOIAGĂ, BEng

Scientific Deputy, Military Equipment and Technologies Research Agency,
Associated Member of Romanian Scientist Academy

DOI: 10.55535/RMT.2025.3.16

The foundational principles of deterrence, largely forged in the crucible of the Cold War's nuclear standoff, are facing an unprecedented stress test in the 21st century. The rapid proliferation of disruptive technologies is fundamentally reshaping the character of warfare, creating new domains of conflict and challenging the efficacy of traditional deterrence models. This paper examines the impact of emerging technologies – including cyberspace operations, artificial intelligence (AI) and autonomous systems, space-based assets and hypersonic weapons – on modern deterrence strategy. It argues that the speed, ambiguity, and asymmetry introduced by these technologies erode the stability of deterrence by punishment and demand a paradigm shift toward a more comprehensive framework. This new framework must integrate deterrence by denial, enhance resilience and leverage all instruments of national power. Through an analysis of recent conflicts and technological trends, this paper provides a series of recommendations for military and policy decision-makers to adapt their strategies to the complex realities of the technological era.

Keywords: deterrence; warfare; emerging technologies; cyberspace; autonomy; space;

INTRODUCTION

The 2022 Russian invasion of Ukraine has served as a stark and brutal reminder that the specter of great power conflict has not been relegated to the annals of history. The war has been a crucible for new technologies and operational concepts, demonstrating the profound impact of unmanned aerial vehicles, sophisticated cyber operations, and the pervasive influence of commercial space technologies on the modern battlefield (CSIS, 2025). The conflict has also exposed the limitations of traditional deterrence strategies. Despite clear and repeated warnings from the United States and its NATO allies, Russia proceeded with its invasion, suggesting a failure of deterrence by punishment. This failure underscores a critical challenge for military and policy decision-makers: the established verities of deterrence, honed during the bipolar nuclear standoff of the Cold War, are proving inadequate in the face of a new technological era.

For decades, deterrence theory rested on a relatively stable foundation. The concept of *Mutually Assured Destruction* (MAD) created a grim but predictable logic that prevented direct conflict between the United States and the Soviet Union. Deterrence was primarily understood as deterrence by punishment – the threat of a devastating retaliatory strike that would inflict unacceptable costs on an aggressor (Freedman, 2020, pp. 1-10). This model, however, is being systematically eroded by a wave of technological innovation. The emergence of new warfighting domains, such as cyberspace and outer space, coupled with the development of artificial intelligence (AI), autonomous systems, and hypersonic weapons, has introduced a level of complexity and ambiguity that traditional deterrence models are not capable to handle.

The central problem is that these new technologies lower the barrier to entry for aggression, create significant attribution challenges and compress decision-making timelines to the point where human cognitive capacity is overwhelmed. A cyberattack can cripple critical infrastructure without a single shot being fired, and its perpetrator can remain shrouded in anonymity (CSIS, 2023). An AI-powered drone swarm could execute a devastating strike in seconds, potentially without direct human intervention (Horowitz, 2021, pp. 764-788). A hypersonic missile, traveling at more than five times the speed of sound, could decapitate a nation's leadership before it has time to react (Finabel, 2021). These are not science fiction scenarios; they are the emerging realities of 21st-century warfare.

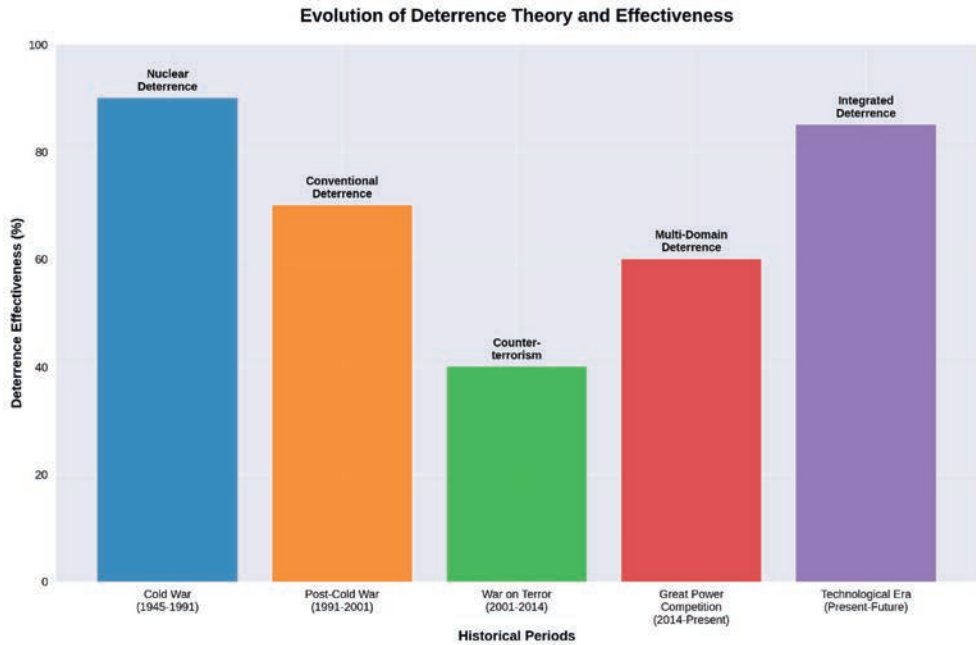


Figure 1: Evolution of deterrence theory and effectiveness across historical periods¹

This paper argues that the NATO and EU member states must fundamentally redefine their approach to deterrence to meet the challenges of the technological era. A strategy predicated solely on the threat of punishment is no longer sufficient. Instead, a more comprehensive framework is required, one that integrates deterrence by denial, enhances national resilience, and leverages all instruments of national power in a coordinated and synchronised manner. This concept, often referred to as “*integrated deterrence*” is not merely a buzzword; it is a strategic imperative.

To advance this argument, this paper will proceed in five parts. First, it will examine the impact of key emerging technologies on the new domains of warfare, including cyberspace, AI and autonomous systems, space, and hypersonic weapons. Second, it will analyse the phenomenon of hybrid warfare and the “*gray zone*”, demonstrating how adversaries are using a combination of conventional and unconventional tactics to achieve their objectives below the threshold of armed conflict. Third, it will draw on case studies from recent conflicts, including the war in Ukraine and the use of AI in Gaza, to illustrate the practical implications

¹ Author’s note: the images were created using AI, based on the text. The data are drawn from the bibliography presented at the end of the article.

of these new technologies for deterrence. Fourth, it will outline a series of policy recommendations for military and policy decision-makers to adapt their strategies to this new reality. Finally, the paper will offer a concluding assessment of the future of warfare and the enduring importance of a credible and effective deterrent.

THE NEW DOMAINS OF WARFARE

The traditional domains of warfare – land, sea, and air have been augmented by new, man-made domains that are increasingly central to military operations and national security.

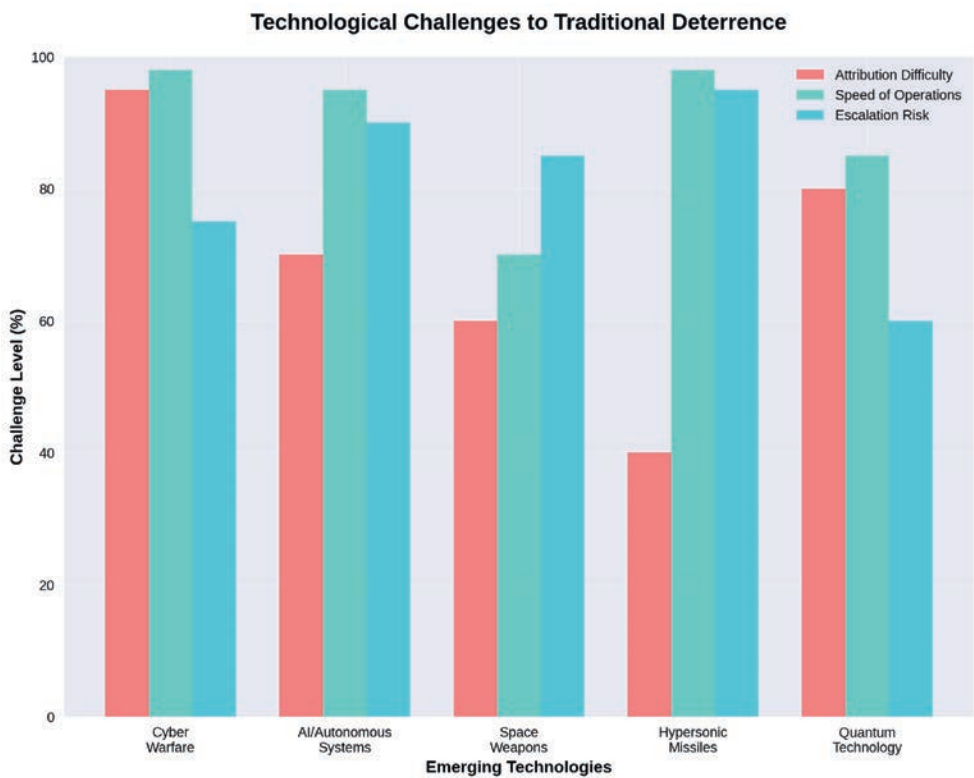


Figure 2: Technological Challenges to Traditional Deterrence Models

Cyberspace and outer space, once considered enabling domains, have become contested warfighting domains in their own right. The proliferation of advanced technologies has created a new reality for military planners and policymakers, one in which the clear distinctions between war and peace are eroding and the potential for rapid, unforeseen escalation is growing.

Cyber Warfare and Deterrence

Cyberspace has emerged as a domain of constant, low-level conflict. State and non-state actors conduct espionage, steal intellectual property, and disrupt critical infrastructure with a degree of anonymity that is unprecedented in the history of warfare. This has profound implications for deterrence. The traditional model of deterrence by punishment, which relies on the ability to credibly threaten retaliation against an aggressor, is difficult to apply in a domain where attribution is often slow, uncertain, and politically fraught (Nye Jr., 2010, pp. 3-14). As the U.S. Congressional Research Service notes, *“cyberspace deterrence strategies seek to influence an adversary’s behaviour, discouraging them from engaging in unwanted activities”* (Congressional Research Service, 2022). However, the very nature of cyberspace makes this a challenging proposition.

The attribution problem is perhaps the most significant challenge to cyber deterrence. It can take weeks or even months to trace a sophisticated cyberattack back to its source, and even then, the evidence may be circumstantial. This ambiguity provides cover for aggressors, allowing them to deny responsibility and avoid retaliation. The use of proxies and non-state actors further complicates the attribution problem, creating a layer of deniability that can be difficult to penetrate (Buchanan, 2016, pp.141-157).

Furthermore, the speed of cyber operations creates a significant challenge for decision-makers. A cyberattack can unfold in milliseconds, leaving little time for deliberation or response. This compressed timeline, coupled with the potential for cascading effects across interconnected systems, creates a risk of rapid, uncontrolled escalation. The concept of *“integrated deterrence”*, as articulated by the U.S. Department of Defense, seeks to address this challenge by leveraging all instruments of national power to deter aggression in cyberspace (NDU Press, May 2023).

This includes not only the threat of a military response but also the use of economic sanctions, diplomatic pressure, and law enforcement actions.

AI and Autonomous Systems

The integration of artificial intelligence (AI) and autonomous systems into military operations represents a paradigm shift in the character of warfare. AI-powered systems can process vast amounts of data, identify targets, and execute attacks at speeds that far exceed human capabilities. This has the potential to create a significant military advantage, but it also introduces a host of new risks and challenges for deterrence and strategic stability.



Figure 3: Autonomous Weapons Systems and AI Integration in Military Operations

One of the most significant concerns is the potential for accidental escalation. As AI systems become more autonomous, there is a risk that they could make decisions that lead to unintended conflict. A 2017 report by the Chatham House noted that *“both military and commercial robots will in the future incorporate ‘artificial intelligence’ (AI) that could make them capable of undertaking tasks and missions on their own”* (Cummings, 2017). This raises the specter of *“flash wars”*, in which autonomous systems engage in a rapid, escalating conflict without meaningful human control. The speed of algorithmic warfare could leave little time for de-escalation or diplomacy, creating a dangerous and unstable dynamic.

The development of lethal autonomous weapons systems (LAWS), or *“killer robots”*, is another area of significant concern. These are weapons that can independently search for, identify, and kill human targets without direct human control. The prospect of ceding life-and-death decisions to a machine raises profound ethical and legal questions (Human Rights Watch, 2012, pp.6-13). It also has significant implications for deterrence. The use of LAWS could lower the threshold for the use of force, as it would remove the risk to human soldiers. This could make it more tempting for states to engage in aggression, undermining the very foundations of deterrence.

Moreover, the proliferation of AI and autonomous systems could lead to a new arms race, as states compete to develop more sophisticated and capable systems. This could create a dangerous and unstable security environment, in which the risk of miscalculation and conflict is high. As a 2024 CSIS report on algorithmic stability notes, *“Information about AI/ML capabilities will influence how states manage*

escalation. Escalation risks will continue to emerge from how warfighting..." (CSIS, 2024).

Space as a Contested Domain

Outer space, once the exclusive domain of a few superpowers, has become increasingly congested, contested, and competitive. The growing reliance on space-based assets for communication, navigation, intelligence, and military operations has made them attractive targets for adversaries. The development of anti-satellite (ASAT) weapons, including co-orbital *"killer satellites"*, directed energy weapons, and ground-based missiles, has created a new and dangerous dimension of warfare (Bingen, 2023, pp.1-33).



Figure 4: Space-Based Assets and Anti-Satellite Warfare Capabilities

The vulnerability of space assets poses a significant challenge to deterrence. A successful attack on a nation's satellites could cripple its military and economic infrastructure, leaving it blind, deaf, and unable to respond effectively to an attack. This creates a powerful incentive for a preemptive strike, as the first mover could gain a decisive advantage. The 2023 RAND Corporation report, *"A Framework of Deterrence in Space Operations"*, emphasises that an effective space deterrence strategy must be tailored to the specific adversary and the phase of the conflict (RAND Corporation, 2023).

The challenges of deterrence in space are compounded by the unique characteristics of the domain. The vastness of space and the high speed of objects

in orbit make it difficult to track and attribute hostile actions. The problem of space debris, which can be created by the destruction of a satellite, poses a threat to all space-faring nations, including the one that created it. This creates a shared interest in avoiding conflict in space, but it also creates a risk of miscalculation and unintended escalation.

The concept of “*space denial*” has emerged as a potential deterrence strategy. This involves developing the capability to deny an adversary the use of its own space assets in a conflict. This could be achieved through a variety of means, including jamming satellite signals, dazzling sensors with lasers, or using cyberattacks to disrupt ground stations. The goal of space denial is not to destroy an adversary’s satellites, but rather to temporarily disrupt their ability to use them. This approach, as outlined in a 2023 NDU Press article, is seen as a less escalatory option than the use of destructive ASAT weapons (NDU Press, October 2023).

Hypersonic Weapons and Strategic Stability

The development of hypersonic weapons, which can travel at speeds in excess of Mach 5, represents another significant challenge to strategic stability. These weapons combine the speed of ballistic missiles with the manoeuvrability of cruise missiles, making them extremely difficult to detect, track, and intercept. This has led some analysts to warn of a new era of vulnerability, in which the traditional pillars of deterrence are undermined (Global Security Review, 2025).

The primary concern is that hypersonic weapons could be used to conduct a disarming first strike against a nation’s nuclear arsenal or leadership. The speed and manoeuvrability of these weapons would make it difficult for a targeted nation to respond in time, potentially leading to a “*use-it-or-lose-it*” dilemma. This could create a dangerous and unstable dynamic, in which both sides are incentivised to strike first in a crisis. A 2021 report by Finabel noted that “*emerging military technologies such as hypersonic weapons challenge the established dynamics of nuclear deterrence and strategic stability*” (Finabel, 2021).

The payload ambiguity of hypersonic weapons further complicates the deterrence calculus. It is difficult to determine whether a hypersonic missile is armed with a conventional or a nuclear warhead until it is too late. This could lead to miscalculation and unintended escalation in a crisis. An adversary might mistake a conventional strike for a nuclear one, leading to a devastating nuclear exchange.

The proliferation of hypersonic weapons could also trigger a new arms race, as states compete to develop their own hypersonic capabilities and defenses.

This could lead to a dangerous and unstable security environment, in which the risk of conflict is high. The Atlantic Council has argued for a clear vision for US hypersonic weapons, emphasising that *“deterrence requires credible, visible capabilities”* (Atlantic Council, 2025). However, the development of these weapons also raises the risk of a destabilizing arms race.

HYBRID WARFARE AND THE GRAY ZONE

The challenges to deterrence are not limited to the emergence of new technologies and warfighting domains. Adversaries are also increasingly operating in the *“gray zone”* between peace and war, using a combination of conventional and unconventional tactics to achieve their objectives without triggering a military response. This phenomenon, often referred to as *“hybrid warfare”* has become a defining feature of 21st-century conflict.

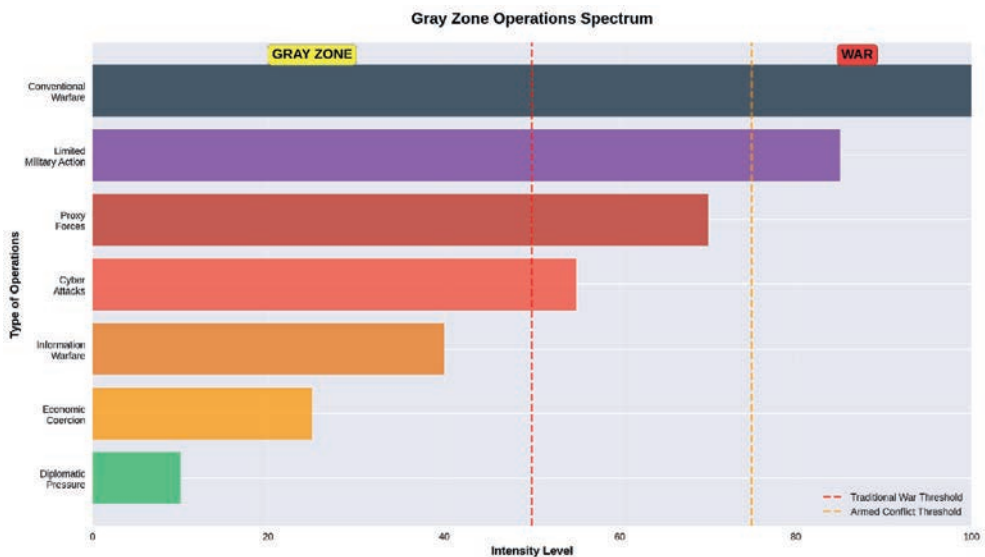


Figure 5: Gray Zone Operations Spectrum – From Peace to War

Hybrid warfare is characterised by the use of a wide range of instruments of power, including disinformation, economic coercion, cyberattacks, and the use of proxies and irregular forces. The goal is to sow confusion, undermine trust in democratic institutions, and create a sense of strategic paralysis. As a 2025 ICRC article notes, terms like *“hybrid threats”* and *“gray zones”* are used to describe *“covert and ambiguous operations, suggesting they blur the lines”* between war and peace (ICRC, 2025).

Russia's actions in Ukraine provide a textbook example of hybrid warfare. Prior to its full-scale invasion in 2022, Russia engaged in a years-long campaign of hybrid warfare, which included the annexation of Crimea, the use of *"little green men"* in the Donbas, and a sustained campaign of disinformation and cyberattacks. These actions were carefully calibrated to remain below the threshold that would trigger a decisive military response from the West.

China has also been accused of engaging in hybrid warfare in the South China Sea. It has used its coast guard and maritime militia to harass and intimidate other claimants, while at the same time engaging in a massive island-building campaign to create a series of unsinkable aircraft carriers. These actions have allowed China to gradually expand its control over the South China Sea without firing a shot.

The challenge of deterring hybrid warfare is that it is often difficult to identify a clear aggressor or a specific act of aggression. The use of proxies and deniable assets makes it difficult to attribute attacks, and the incremental nature of many hybrid warfare campaigns makes it difficult to justify a military response. This creates a significant challenge for policymakers, who must find a way to deter aggression without escalating to a full-blown conflict. A 2025 *Small Wars Journal* article highlights the need for a framework to measure hybrid warfare, noting that it *"lacks clear definitions"* (Small Wars Journal, 2025).

POLICY IMPLICATIONS AND RECOMMENDATIONS

The profound shifts in the character of warfare demand a commensurate shift in how the United States and its allies approach deterrence. A reliance on Cold War-era models is a recipe for strategic failure. To effectively deter aggression in the 21st century, policymakers and military leaders must embrace a new framework for deterrence, one that is more comprehensive, integrated, and agile. This section outlines a series of policy recommendations designed to achieve that goal.

Redefining Deterrence: From Punishment to a Comprehensive Approach

The cornerstone of a modern deterrence strategy must be a move away from an over-reliance on deterrence by punishment. While the threat of retaliation remains a critical component of deterrence, it is no longer sufficient on its own. A more comprehensive approach is needed, one that also incorporates deterrence by denial, resilience, and cost imposition.

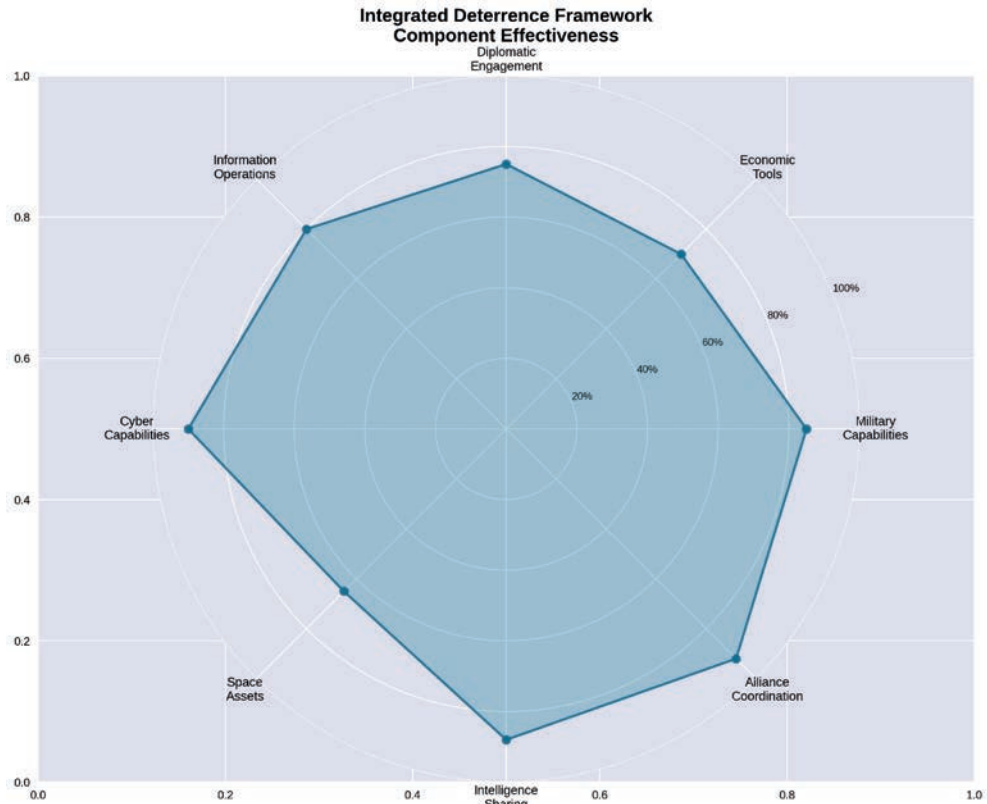


Figure 6: Integrated Deterrence Framework - Multi-Domain Approach

- **Deterrence by Denial:** This involves convincing an adversary that they will not be able to achieve their objectives on the battlefield. This can be achieved through a variety of means, including the development of advanced military capabilities, the hardening of critical infrastructure, and the use of new operational concepts. The goal is to create a credible defence that will deny an aggressor the prospect of a quick and easy victory.
- **Resilience:** In an era of persistent, low-level conflict, it is no longer possible to prevent all attacks. Therefore, it is essential to build a resilient society that can withstand and recover from an attack. This includes everything from hardening critical infrastructure against cyberattacks to developing a robust civil defence program.
- **Cost Imposition:** This involves imposing costs on an adversary for their aggressive behaviour, even if it falls below the threshold of armed conflict. This can be achieved through a variety of means, including economic

sanctions, diplomatic isolation, and law enforcement actions. The goal is to make it clear that there will be consequences for aggression, even if it does not trigger a military response.

Integrated Deterrence: A Whole-of-Government Approach

The concept of integrated deterrence, as articulated in the 2022 US National Defense Strategy, is a critical component of a modern deterrence strategy. It recognises that military power is only one instrument of national power, and that a truly effective deterrent requires the integration of all instruments of power, including diplomatic, economic, and informational.

This requires a whole-of-government approach to deterrence, in which all agencies and departments are working together to achieve a common set of objectives. It also requires close coordination with allies and partners, who are essential to building a broad coalition to deter aggression.

Technological Superiority: The Race for the High Ground

In an era of rapid technological change, maintaining a technological edge is more important than ever. The NATO and EU member states must continue to invest in research and development to ensure that they have the most advanced military capabilities in the world. This includes everything from developing new AI-powered systems to building more resilient space assets.

However, technological superiority is not just about having the best hardware. It is also about having the best people. The NATO and EU member states must invest in the education and training of their military personnel to ensure that they have the skills and knowledge to operate in a complex and rapidly changing security environment.

Arms Control and Norms: Building Guardrails for a New Era

The development of new and disruptive technologies has created a pressing need for new arms control agreements and international norms. The existing arms control framework, which was designed for the Cold War, is ill-equipped to deal with the challenges of the 21st century. New agreements are needed to govern the development and use of AI, autonomous systems, and hypersonic weapons.

In addition to formal arms control agreements, there is also a need to develop new international norms of behaviour. This includes everything from establishing rules of the road for cyberspace to developing a code of conduct for military operations in outer space. The goal is to create a more stable and predictable security environment, in which the risk of miscalculation and conflict is reduced.

Professional Military Education: Preparing Leaders for the Future of War

Finally, it is essential to reform professional military education to prepare leaders for the challenges of the 21st century. Military leaders must have a deep understanding of the implications of new technologies for warfare and deterrence. They must also be able to think critically and creatively about how to solve complex security problems.

This will require a new approach to professional military education, one that emphasizes interdisciplinary learning, critical thinking, and a deep understanding of the changing character of warfare. It will also require a greater emphasis on wargaming and simulation, to give leaders the opportunity to test new concepts and ideas in a realistic and challenging environment.

CONCLUSIONS

The technological tsunami of the 21st century has washed away the familiar landmarks of the Cold War deterrence landscape. The emergence of cyberspace and outer space as warfighting domains, coupled with the development of artificial intelligence, autonomous systems, and hypersonic weapons, has created a new and dangerous security environment. The old verities of deterrence, which were based on the threat of a devastating nuclear exchange, are no longer sufficient to deter aggression in an era of hybrid warfare and gray zone conflict.

This paper has argued that the NATO and EU member states must fundamentally redefine their approach to deterrence to meet the challenges of the technological era. A strategy predicated solely on the threat of punishment is a recipe for strategic failure. Instead, a more comprehensive framework is required, one that integrates deterrence by denial, enhances national resilience, and leverages all instruments of national power in a coordinated and synchronised manner.

The policy recommendations outlined in this paper provide a roadmap for how to achieve this goal. They include a call for a new, more comprehensive approach to deterrence; a greater emphasis on integrated deterrence; a sustained investment in technological superiority; a renewed focus on arms control and international norms; and a reform of professional military education. These recommendations are not a panacea, but they do provide a starting point for a much-needed debate about the future of deterrence in the 21st century.

Ultimately, the challenge of redefining deterrence is a challenge of imagination. It requires policymakers and military leaders to think creatively about how to deter aggression in a world where the lines between peace and war are increasingly

Technology Domain	Key Challenges	Deterrence Impact	Policy Response
Cyber Warfare	Attribution difficulty Speed of operations Non-state actors	High - Undermines retaliation credibility	Integrated cyber deterrence Active defense International norms
AI/Autonomous Systems	Flash wars Ethical concerns Accidental escalation	Very High - Removes human control	Human-in-the-loop requirements AI arms control Ethical guidelines
Space Domain	Debris creation Dual-use technology Attribution challenges	High - Critical infrastructure vulnerability	Space denial strategies International agreements Resilience building
Hypersonic Weapons	Payload ambiguity Compressed timelines Defense penetration	Very High - First strike advantage	Early warning systems Defensive capabilities Arms control
Hybrid/Gray Zone	Below-war threshold Deniability Incremental nature	Medium - Gradual erosion of deterrence	Whole-of-government response Cost imposition Resilience measures

Table 1: Summary of Technological Challenges to Deterrence and Policy Responses

blurred. It requires a willingness to question old assumptions and to embrace new ideas. And it requires a recognition that the future of warfare will be determined not only by the technologies we develop, but also by the strategies we devise to use them.

BIBLIOGRAPHY:

1. Atlantic Council (19 August 2025). *A Vision for US Hypersonic Weapons*, <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/a-vision-for-us-hypersonic-weapons/>, retrieved on 2 September 2025.
2. Bingen, K.A., Johnson, K., Young, M. (2023). *Space Threat Assessment 2023*, Center for Strategic and International Studies/CSIS, pp.1-33.
3. Buchanan, B. (2017). *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*, Oxford University Press.
4. Congressional Research Service (18 January 2022). *Cybersecurity: Deterrence Policy*, <https://www.congress.gov/crs-product/R47011/>, retrieved on 26 August 2025.
5. Center for Strategic and International Studies/CSIS (15 November 2023), *Deterrence and Cyber Strategy*, <https://www.csis.org/analysis/deterrence-and-cyber-strategy/>, retrieved on 12 August 2025.
6. Center for Strategic and International Studies/CSIS (10 June 2024). *Algorithmic Stability: How AI Could Shape the Future of Deterrence*, <https://www.csis.org/analysis/algorithmic-stability-how-ai-could-shape-future-deterrence/>, retrieved on 2 September 2025.
7. Center for Strategic and International Studies/CSIS (2 May 2025). *Lessons from the Ukraine Conflict: Modern Warfare in the Age of Autonomy, Information, and Resilience*, <https://www.csis.org/analysis/lessons-ukraine-conflict-modern-warfare-age-autonomy-information-and-resilience/>, retrieved on 12 August 2025.
8. Cummings, M. (26 January 2017). *Artificial Intelligence and the Future of Warfare*, Chatham House, <https://www.chathamhouse.org/sites/default/files/publications/research/2017-01-26-artificial-intelligence-future-warfare-cummings-final.pdf>, retrieved on 29 August 2025.
9. Finabel (9 February 2021). *The Strategic Implications of Hypersonic Weapons*, <https://finabel.org/the-strategic-implications-of-hypersonic-weapons/>, retrieved on 20 August 2025.
10. Freedman, L. (2020). *The Evolution of Deterrence Strategy and Research*, in NL ARMS Netherlands Annual Review of Military Studies, DOI:10.1007/978-94-6265-419-8_1, pp.1-10.
11. Global Security Review (5 May 2025). *Hypersonic Weapons: Are We Entering a New Era of Vulnerability?*, <https://globalsecurityreview.com/hypersonic-weapons-are-we-entering-a-new-era-of-vulnerability/>, retrieved on 10 September 2025.
12. Horowitz, M.C. (2021). *When Speed Kills: Lethal Autonomous Weapon Systems, Deterrence and Stability*, in *Emerging Technologies and International Stability*, ed. Michael Krepon, Taylor&Francis, pp.764-788.
13. Human Rights Watch (19 November 2012). *Losing Humanity: The Case against Killer Robots*, ISBN: 1-56432-964-X, pp.6-13.

14. ICRC (16 January 2025). *'Hybrid Threats', 'Grey Zones', 'Competition', and 'Proxies': When Is It Actually War?*, <https://blogs.icrc.org/law-and-policy/2025/01/16/hybrid-threats-grey-zones-competition-and-proxies-when-is-it-actually-war/>, retrieved on 5 September 2025.
15. NDU Press (4 May 2023). *Cyber Deterrence Is Dead! Long Live 'Integrated Deterrence'!*, <https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3379791/cyber-deterrence-is-dead-long-live-integrated-deterrence/>, retrieved on 26 August 2025.
16. NDU Press (30 October 2023). *Space Denial: A Deterrence Strategy*, <https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3569640/space-denial-a-deterrence-strategy/>, retrieved on 27 August 2025.
17. Nye Jr., J.S. (May 2010). *Cyber Power*, Belfer Center for Science and International Affairs, Harvard Kennedy School.
18. RAND Corporation (31 August 2023). *A Framework of Deterrence in Space Operations*, https://www.rand.org/pubs/research_reports/RRA820-1.html, retrieved on 2 September 2025.
19. Small Wars Journal (17 June 2025). *Quantifying the Gray Zone: A Framework for Measuring Hybrid Warfare*, <https://smallwarsjournal.com/2025/06/17/framework-for-hybrid-warfare/>, retrieved on 10 September 2025.

EMERGING TECHNOLOGIES AND NATO'S EASTERN FLANK: PERSPECTIVES FOR ROMANIA

Captain Cătălin-Costel DUMITRIU

"Nicolae Bălcescu" Land Forces Academy, Sibiu

DOI: 10.55535/RMT.2025.3.17

This article examines how emerging technologies are reshaping security and defence on NATO's Eastern Flank, with particular attention to Romania. Building on a five-dimension analytical framework – command and control (C2), intelligence and situational awareness (ISR), decision speed, operational agility, and systemic resilience – originally distilled from Ukraine's experience, the study adapts and applies this grid to Romanian realities. Methodologically, it is qualitative and exploratory, triangulating specialised literature, NATO doctrinal documents, and close observation of recent developments in the Russia-Ukraine war. Findings identify vulnerabilities in C2 infrastructure, logistics, and cyber resilience, alongside opportunities stemming from the accelerated integration of autonomous systems, digital infrastructures, and AI-assisted decision processes. The conclusions underscore the strategic salience of technological emergence for strengthening deterrence and defence, enhancing interoperability, and consolidating Romania's position as a pivotal state within NATO's regional security architecture.

Keywords: emerging technologies; Eastern Flank; decision speed; operational agility; resilience;

INTRODUCTION

The full-scale military aggression launched by the Russian Federation against Ukraine in February 2022 functioned as a genuine catalyst for re-evaluating traditional security and defence paradigms across Europe and the wider Euro-Atlantic community. Unlike earlier conventional conflicts, this war has demonstrated in real time that emerging technologies are not a marginal enabler but a decisive vector of operational resilience and strategic adaptiveness. The extensive use of uncrewed aerial systems, secure communications architectures, AI-enabled decision-support platforms, and open-source intelligence (OSINT) instruments has validated the hypothesis that technological innovation can significantly recalibrate the balance of power even under pronounced resource asymmetries.

For the states located on NATO's Eastern Flank, including Romania, the ongoing conflict constitutes a strategic laboratory with far-reaching implications. Geographic proximity, the structural vulnerability of the Black Sea region, and Romania's status as a pivot state within the allied defensive architecture entail heightened exposure but also augmented strategic responsibility. Under these conditions, it becomes imperative that the lessons distilled from Ukraine's experience should be translated into coherent defence policies, modernised doctrine, and operational practices tailored to national specificities yet fully compatible with NATO standards and mechanisms.

The purpose of this study is to analyse the impact of emerging technologies on security and defence along NATO's Eastern Flank, with a particular focus on Romania. To this end, it deploys a multidimensional analytical framework developed in the specialised literature and structured around five dimensions essential to operational success: (1) *command and control*; (2) *intelligence and situational awareness*; (3) *decision speed*; (4) *operational agility*; and (5) *systemic resilience*. This framework enables both a comprehensive appraisal of current preparedness and the identification of strategic development pathways.

Methodologically, the study is qualitative and exploratory, grounded in the triangulation of multiple sources: a comparative analysis of the specialised literature; an assessment of NATO doctrinal documents (Strategic Concept 2022; NATO Warfighting Capstone Concept 2021); and a critical examination of recent developments generated by the Ukrainian conflict. This design provides robust anchoring, ensuring both theoretical validity and practical salience of the findings.

The research is relevant, in theoretical terms, by contributing to the consolidation of the literature on the technological revolution in the military domain and on contemporary evolutions in the art of war and, in practical terms, by formulating actionable recommendations aimed at strengthening institutional resilience, modernising doctrine, and consolidating Romania's interoperability within NATO.

In an era defined by strategic volatility, uncertainty, and systemic complexity, the emergence of new technologies is part of a broader paradigmatic transformation of warfare commonly associated in the literature with the *Revolution in Military Affairs (RMA)*. Whereas in the past technological change manifested primarily through the introduction of technically superior weapon platforms, contemporary reality points to a transgression of traditional boundaries. Today, innovation is not reducible to procurement alone; it presupposes the simultaneous integration of digital infrastructures, artificial-intelligence algorithms, big-data analytics, and cyber-resilience mechanisms, elements that converge to reconfigure the nexus between military power and strategic competitiveness.

This epistemic shift obliges NATO member states, and Romania in particular, to move beyond incrementalist modernisation and adopt a proactive, anticipatory, and systemic approach. National security on the Eastern Flank can no longer be conceptualised solely in terms of force mass or conventional capabilities; it must be grounded in digital interoperability, decentralised command architectures, and organisational cultures that incentivise rapid innovation.

Accordingly, the present analysis seeks to contribute to the institutionalisation of an academic and doctrinal debate on how Romania can leverage recent Ukrainian lessons to configure a robust strategic profile. At the same time, the article aligns with NATO's strategic-planning documents, which underscore technological emergence not only as an opportunity but also as a critical determinant of institutional survivability and operational effectiveness. In this reading, the Eastern Flank becomes not merely a defensive perimeter but a testbed for the Alliance's adaptiveness to the new conditions of contemporary conflict. Consequently, the study aspires to serve as an analytic benchmark for understanding how Romania and NATO can convert technological emergence into a vector of long-lasting security and stability.

EMERGING TECHNOLOGIES IN DEFENCE: AN ANALYTICAL FRAMEWORK

In analysing the metamorphoses of contemporary warfare, it becomes evident that emerging technologies operate not as mere power multipliers but as structural determinants of the operational architecture. Beyond sheer technicity,

they configure a veritable epistemic mutation of war, wherein knowledge, velocity, and adaptiveness become the defining vectors of military effectiveness. Within this horizon, the proposal of an integrative analytical framework, articulated along five dimensions – command and control (C2), intelligence and situational awareness (ISR), decision speed, operational agility, and systemic resilience, enables not only a synoptic comprehension of the phenomenon but also the operationalisation of the *Revolution in Military Affairs (RMA)* in an application-oriented key, tailored to NATO as well as Romania-specific exigencies.

Command and Control (C2)

The C2 dimension transcends the traditional logic of rigid hierarchical chains, being reconfigured by the emergence of distributed information ecologies marked by redundancy, resilience, and persistent interconnectivity. Whereas previous conflicts privileged the vertical transmission of orders, contemporary warfare evidences the prevalence of networked, adaptive, and decentralised architectures.

Illustratively, the use of the Starlink network in Ukraine has shown that access to resilient, dispersed communications infrastructures can radically reshape conflict dynamics by preserving C2 continuity even amid the degradation of conventional infrastructure (Kofman, Lee, 2022, pp. 10-18). Artificial intelligence contributes to multisource data fusion and the generation of a Common Operational Picture, facilitating the simultaneous synchronisation of distributed actors (Alberts, Garstka, Stein, 1999, pp. 45-62).

For Romania, the challenge lies in integrating national C2 infrastructures into NATO's allied meta-systems. In the absence of accelerated modernisation, the state risks becoming a “*weak node*” in the network. The remedy entails end-to-end digitalisation of decision chains, the deployment of secure cloud architectures, and the cultivation of a mission-command leadership doctrine capable of operating in tandem with automated systems (NATO, 2021, p. 27).

Intelligence and Situational Awareness (ISR)

ISR has become the centre of gravity of modern conflict, wherein information superiority precedes and conditions operational superiority. The diffusion of emerging technologies has created the premises for a form of operational near-omniscience, as the boundaries between theatres of operations, the cyber domain, and the cognitive domain progressively dissolve.

Today, distributed sensor networks, militarised commercial drones, private Earth-observation satellite constellations, and OSINT instruments coalesce into a markedly democratised ISR ecosystem, one in which even non-state actors can

field capabilities approximating those of major powers (Horowitz, 2018, pp. 40-45). It erodes the state's erstwhile information monopoly and compels the introduction of novel mechanisms for data triage, validation, and integration.

In the Black Sea region, Romania operates within a contested environment where Russian electronic warfare and A2/AD (anti-access/area-denial) complexes constrain ISR freedom of action (Mareš, 2022, pp. 5-19). Even so, participation in NATO information-sharing mechanisms, such as the NATO Intelligence Fusion Centre, can mitigate national shortfalls. Accordingly, Romania should invest in multisource ISR fusion and contribute proactively to building a regional Common Operational Picture (regional COP).

Decision Speed

In an era of *"hyper-temporality"* in warfare, strategic advantage accrues to the actor capable of compressing OODA loops through digital instruments and artificial intelligence. If the twentieth century privileged mass and volume, today the decisive variable is cognitive tempo – the speed at which information is transmuted into action.

Predictive systems, big-data analytics, and AI-based decision-support tools recast decision-making as a simultaneous, distributed, and anticipatory process. Ukrainian practice demonstrates that decision speed can offset numerical or material inferiority (Watling, Reynolds, 2022, pp. 42-51).

For Romania, the challenge is twofold: technological – integrating decision-support systems within C2; and cultural – cultivating an adaptive organisational ethos that reduces bureaucratic inertia. Within NATO, decision speed is a critical criterion of interoperability: a slow-reacting partner can desynchronise the Alliance as a whole (NATO, 2022, p. 14).

Operational Agility

Operational agility denotes the armed forces' capacity to reconfigure structures and procedures instantaneously in response to the dynamics of the operational environment. It is enabled by platform modularity, decentralised logistics, and the employment of autonomous units. Agility is not mere flexibility; it presupposes a form of institutional plasticity through which forces can exploit ephemeral opportunities and neutralise emergent threats.

Recent cases indicate that network-enabled military structures, operating with decentralised, autonomous formations, can maintain initiative even against numerically superior adversaries (Murray, Knox, 2001, pp. 196-201). For Romania, agility entails a doctrinal mutation from a linear, volume-centric model to a multi-domain, distributed paradigm optimised for decentralised, contested operations.

Systemic Resilience

Resilience constitutes the cardinal dimension of strategic survivability. It denotes the capacity to maintain critical functions under maximal stress, even amid systemic degradation. Unlike tactical resilience, which centres on discrete units or equipment, systemic resilience encompasses the entire national and allied ecosystem: critical infrastructures, energy grids, communications, logistics chains, and societal cohesion.

In Ukraine, the adaptation of civilian infrastructures for military purposes – most saliently, redundant energy networks – has underscored the indispensability of fusing military and societal resilience (Reznikova, 2022, pp. 45-63). For Romania, positioned along the Eastern Flank's contact line, consolidating resilience requires the integration of civil-military efforts, the protection of critical infrastructures, and the institutionalisation of a whole-of-society resilience framework capable of sustaining national defence over the long term (Radin, 2023, p. 31).

Relevance for NATO and Romania

The five-dimension framework aligns with NATO's priorities as articulated in the Strategic Concept 2022 and the NATO Warfighting Capstone Concept 2021, wherein information superiority, multi-domain agility, and collective resilience are identified as decisive determinants of institutional survivability (NATO, 2022, pp. 7-10; NATO, 2021, p. 27).

For NATO, the model provides an operational grid of doctrinal convergence; for Romania, it constitutes a precondition of strategic credibility, indispensable to consolidating its role as a pivot state on the Eastern Flank. The internalisation of this framework amounts to a paradigmatic leap – from incremental modernisation to anticipatory, system-level integration within the Euro-Atlantic security architecture (Radin, 2023, pp. 29-32).

ROMANIA ON NATO'S EASTERN FLANK

Geostrategic Position and Romania's Role in Collective Security

Romania constitutes a veritable geostrategic node within the Euro-Atlantic security architecture by virtue of its location at the confluence of Central Europe, the Balkans, and the Pontic space. The Eastern Flank, of which Romania is an integral component, is today not merely a peripheral defensive zone but an epicentre of contestation between the liberal international order and the Russian Federation's revisionist dynamics (Barros, 2023, pp. 7-10).

Romania's access to the Black Sea and immediate proximity to Ukraine, the Republic of Moldova, and the wider Caucasus endow it with a pivot-state role within the Alliance. Its status as host to critical capabilities, such as the Aegis Ashore system at Deveselu and multinational command-and-control structures (NATO Force Integration Units, HQ MNC-SE), amplifies its salience as a regional security provider and a pole for the projection of collective deterrence (NATO, 2022, pp. 14-16). In this regard, Romania becomes a *"geopolitical hinge"* between the Euro-Atlantic and Eurasian spaces, with its national resilience mapping directly onto NATO's collective resilience.

Structural Vulnerabilities

Notwithstanding this strategic positioning, Romania continues to exhibit structural vulnerabilities that may attenuate the effectiveness of its contribution to collective defence.

Command and Control (C2) remains partly beholden to fragmented, insufficiently digitalised conventional infrastructures, which complicates full integration into NATO's networked meta-systems (Alberts, Garstka, Stein, 1999, pp. 52-54). The absence of distributed architectures predicated on redundancy and digital hardening heightens the risk of Romania becoming a point of fragility within the Alliance's command chain.

National logistics, especially transport infrastructure, faces significant constraints. Constrained rail networks, a Port of Constanța susceptible to blockages, and insufficiently modernised road infrastructure diminish strategic mobility and the capacity to sustain logistics flows under conditions of high-intensity conflict (Ti, Kinsey, 2023, pp. 28-31). This structural fragility amplifies dependence on allied support and regional logistics corridors.

In cybersecurity, despite hosting the European Cybersecurity Competence Centre, Romania remains subject to persistent cyberattacks attributed to hostile state actors (Reznikova, 2022, pp. 50-52). A deficit of unified organisational culture and an institutional fragmentation constrain the cohesion of efforts, thereby undermining digital resilience in an environment where hybrid and cyber warfare have become permanent dimensions of contestation.

Ongoing Initiatives

To counteract these vulnerabilities, Romania has embarked upon a complex, multidimensional programme of military, doctrinal, and institutional modernisation.

On the axis of conventional capabilities, acquisition programmes for F-16 multirole aircraft and the future F-35 fleet, the integration of Patriot and HIMARS

systems, as well as naval modernisation exemplify the shift from a territorially oriented defence force to a multi-domain, interoperable force aligned with NATO standards (Kofman, Lee, 2023, pp. 22-26).

At the allied level, Romania contributes actively to strengthening NATO's deterrence-and-defence posture by hosting multinational forces, participating in large-scale exercises such as *"Defender Europe"*, and integrating into initiatives like Enhanced Forward Presence and Tailored Forward Presence (NATO, 2021, p. 34). These endeavours buttress the credibility of Romania's commitment to act as a security provider, not merely a beneficiary.

In the cyber-technological sphere, Romania is consolidating partnerships with the EU and NATO through the European Cybersecurity Competence Centre and participation in Smart Defence initiatives oriented toward innovation and cost-sharing (Galeotti, 2022, pp. 113-115). Taken together, these initiatives evince a paradigmatic shift from traditional defence to comprehensive security grounded in societal resilience and the integration of emerging capabilities.

Applied Analysis by Dimensions

❖ Command and Control (C2): Integration with NATO, Digitalisation, Infrastructure

Within the paradigm of contemporary conflict, C2 transcends the linear logic of rigid hierarchical chains and is reconstituted as a distributed information ecosystem characterised by redundancy and persistent interconnectivity (Alberts, Garstka, Stein, 1999, pp. 52-54). For Romania, integration into NATO's command meta-systems requires not only technical interoperability but also doctrinal convergence with the mission command principle, whereby local leaders exercise devolved decision authority under conditions of uncertainty.

Current limitations derive from an excessive reliance on conventional, only partially digitalised infrastructures, vulnerable to cyber or kinetic attack. Ukraine's experience has shown that decentralised networks (e.g., Starlink) can preserve C2 functionality even amid systemic degradation. Through its integration with the NATO Communications and Information Agency (NCIA), Romania must accelerate the end-to-end digitalisation of decision chains, including the deployment of secure tactical clouds and AI-based systems for multisource data fusion.

Poland has achieved a more advanced C2 integration into NATO meta-systems, benefiting from robust infrastructure and consolidated partnerships with the United States of America (including the Redzikowo site). By contrast, the Baltic states, though smaller, have compensated through accelerated digitalisation and mission-command doctrines. Romania remains partly dependent on conventional

infrastructures, necessitating a transition toward secure cloud architectures and distributed designs to avoid becoming a “*vulnerable node*” within the allied network (Ib.).

❖ **Intelligence and Situational Awareness (ISR): Drones, Satellites, OSINT, Analysis Centres**

ISR has become the centre of gravity of modern conflict, wherein information superiority precedes and conditions operational superiority (Horowitz, 2018, pp. 38-40). The war in Ukraine has showcased the potential of militarised commercial drones, commercial satellite constellations (Maxar, Planet Labs), and OSINT, employed for the rapid verification and geolocation of targets.

Romania operates within a contested electromagnetic environment in which the Russian Federation fields advanced electronic-warfare capabilities and A2/AD systems emplaced in Crimea (Watling, Reynolds, 2022, pp. 12-15). Integration with the NATO Intelligence Fusion Centre and the expansion of partnerships with the private sector are therefore imperative to securing a Common Operational Picture. Romania must also develop national multisource analysis centres capable of ingesting and fusing high-volume data streams from drones, satellites, and OSINT feeds while avoiding cognitive oversaturation.

The Baltic states excel through the integration of OSINT and civic sensor networks into their national architectures, leveraging private-sector partnerships and a high level of digital literacy. Poland has invested heavily in indigenous drone and satellite programmes, cultivating partnerships with the United States of America and France. Romania remains vulnerable to Russian electronic contestation in the Black Sea and relies on NATO information-sharing to obtain a Common Operational Picture (Ib.).

❖ **Decision Speed: Leadership, AI, Accelerated Processes**

In a strategic environment defined by hyper-temporality, advantage accrues to the actor capable of compressing OODA cycles through technology and an adaptive organisational culture (Krepinevich, 1992, pp. 19-21). Whereas in the past superiority derived from mass and volume, today it hinges on cognitive tempo, namely the ability to translate information into action faster than the adversary.

Romania requires a cultural reform of military leadership, moving from a bureaucratic model to an anticipatory, decentralised one. The integration of AI instruments – from logistics-forecasting algorithms to predictive systems for battlespace analytics – can attenuate decision inertia and enhance responsiveness. Within NATO, decision speed is not an individual attribute but a condition of interoperability: a slow-reacting state can desynchronise the Alliance as a whole (Biddle, Friedman, 2022, pp. 9-12).

Poland has embraced a proactive doctrine and a leadership culture grounded in decentralisation, enabling rapid reaction. The Baltic states, by virtue of compact force structures and a territorial-defence orientation, have developed swift, flexible decision mechanisms. Romania remains partly constrained by bureaucratic inertia, which retards decision processes; integrating AI and predictive tools is essential to narrow this gap (Ib.).

❖ **Operational Agility: Mobility, Logistics, Modularity**

Agility denotes the institutional plasticity of the armed forces to reconfigure themselves instantaneously in response to the dynamics of the operational environment (Murray, Knox, 2001, pp. 67-70). In Ukraine, modular structures and autonomous units have demonstrated that agility can offset an adversary's numerical superiority.

For Romania, this dimension is critical: constrained logistics infrastructure (rail networks, bridges, ports) impairs force mobility. Modernisation projects (Rail2Sea and Via Carpathia) must be accelerated to create strategic mobility corridors. Furthermore, military doctrine should privilege multi-domain operations with distributed, autonomous, and interlinked units capable of exploiting ephemeral opportunities.

Poland benefits from extensive logistics corridors and infrastructures that enable rapid strategic mobility, functioning as the principal support hub for Ukraine. The Baltic states, by contrast, compensate for limited infrastructure through modular force design and dispersed formations, thereby enhancing resilience. Romania, given deficient rail and road infrastructure, must expedite Rail2Sea and Via Carpathia to ensure allied mobility on the southern tier of the Eastern Flank (Ti, Kinsey, 2023).

❖ **Systemic Resilience: Cyber, Critical Infrastructures, Societal Resilience**

Resilience is not reducible to the tactical level; it constitutes the backbone of strategic survivability. It entails the maintenance of critical functions under systemic shock – from energy infrastructures and communications to societal cohesion (Reznikova, 2022, pp. 46-49).

In Ukraine, the fusion of civilian and military infrastructures – for example, the adaptation of energy networks and the integration of OSINT into official structures – has demonstrated that societal resilience is inseparable from military resilience. For Romania, vulnerabilities within critical infrastructures (energy, transport, communications) necessitate a whole-of-society strategy, in which civil institutions, the private sector, and citizens collectively participate in reinforcing national resilience.

Moreover, by hosting the European Cybersecurity Competence Centre (ECCC), Romania has the opportunity to become a regional hub of digital resilience, integrated into NATO’s cyber-defence strategy.

The Baltic states are widely considered models of societal resilience: their governments have developed Total Defence programmes that integrate the civilian population into the security architecture. Poland has invested heavily in critical infrastructures and cybersecurity, consolidating its resilience capacity. Romania, although hosting the ECCC, remains vulnerable to hybrid attacks and institutional fragmentation, making a whole-of-society strategy indispensable for knitting together military and societal resilience (Reznikova, 2022).

To complete the multidimensional analysis, *table 1* provides a comparative synthesis of the positioning of Romania, Poland, and the Baltic states, highlighting both areas of doctrinal and institutional convergence and the structural vulnerabilities specific to each state.

Table 1: Comparative Analysis by Dimensions (Romania – Poland – the Baltic States) (author’s design)

Dimension	Romania	Poland	The Baltic States
C2 (Command and Control)	Partially digitalised infrastructures; incomplete integration into NATO meta-systems; risk of a “weak node”	Advanced integration with the USA and NATO (e.g., Redzikowo); robust infrastructure	Distributed architectures; accelerated digitalisation; mission-command doctrine
ISR (Intelligence and Situational Awareness)	Vulnerability to Russian electronic warfare in the Black Sea; reliance on NATO information-sharing	Investments in drones and satellites; strategic partnerships with the USA and France	OSINT and civic-sensor integration; high digital literacy
Decision (Decision Speed)	Slow bureaucratic processes; insufficient AI integration; rigid organisational culture	Decentralised leadership; anticipatory and proactive processes	Compact structures; flexible mechanisms; rapid reactions

Dimension	Romania	Poland	The Baltic States
Agility (Mobility and Logistics)	Deficient infrastructure (rail, road, port); Rail2Sea and Via Carpathia projects underway	Principal logistics hub for Ukraine; extensive infrastructures	Modular, dispersed structures; logistical resilience through dispersal
Resilience (Cyber, Critical Infrastructures, Societal)	Cyber and institutional vulnerabilities; societal fragmentation; potential via the European Cybersecurity Competence Centre (ECCC)	Major investments in critical infrastructures and cyber; consolidated resilience	Total Defence models; societal integration in defence; high cohesion

Table 1 indicates that Poland occupies the position of regional leader by virtue of robust infrastructures and advanced integration with NATO, whereas the Baltic states constitute a testbed of societal and digital resilience. Romania holds an intermediate posture: despite its pivot-state status on the Black Sea, persistent vulnerabilities endure in infrastructure, C2, and cyber resilience. Accordingly, consolidating digital interoperability, accelerating logistical mobility, and institutionalising a whole-of-society strategy become imperatives for transforming Romania from a “vulnerable node” into a key actor of collective security.

IMPLICATIONS FOR NATO AND ROMANIA

Romania’s Alignment with the NATO Strategic Concept (2022) and the NATO Warfighting Capstone Concept (2021)

The NATO Strategic Concept adopted in Madrid (2022) marked a paradigmatic shift: Russia is explicitly designated a direct threat, while China is identified as a systemic rival. This re-conceptualisation of the strategic environment mandates an unprecedented reinforcement of the Eastern Flank. In parallel, the NATO Warfighting Capstone Concept (2021) anticipates the 2040 security environment and introduces multi-domain operations (MDO) as the new organising schema of military thought, emphasising convergence across the land, air, maritime, cyber, and space domains (NATO, 2021, pp. 12-15).

For Romania, alignment entails:

- *Doctrinal transformation: a transition from a linear, territorially focused defence model to an anticipatory, multi-domain architecture, with primacy accorded to interoperability and the integration of emerging technologies;*
- *Infrastructural modernisation: Romania's role as a logistics and strategic hub in the Black Sea compels substantial investment in critical infrastructures (ports, rail corridors, and a secured airspace);*
- *Pivot role in regional security: unlike Poland (the Northern hub) and the Baltic states (forward outposts), Romania is the southern bastion of the Eastern Flank, which confers upon it the responsibility to underwrite cohesion across the Alliance's southern tier.*

Romania's Practical Contributions to Regional Security

Romania does not merely receive security from NATO; it also projects security through:

- **Multinational structures:** Romania hosts the Headquarters Multinational Division South – East (HQ MNC-SE) and NATO Force Integration Units (NFIU) – institutional keystones for rapid planning and deployment.
- **Ballistic-missile defence capability:** The Aegis Ashore site at Deveselu forms an integral component of NATO's ballistic missile defence, rendering Romania both a strategic target and a provider of allied security.
- **Multinational exercises:** Participation in – and hosting of – large-scale exercises such as Defender Europe, Saber Guardian, and Sea Breeze demonstrate Romania's capacity to ensure operational interoperability.
- **Energy and infrastructure initiatives:** The BRUA corridor and Neptun Deep project bolster energy independence and regional security, diminishing reliance on Russian gas.

Through these contributions, Romania functions as an integrated security node on the Black Sea, complementing Poland's role on the Baltic axis.

Lessons for Interoperability and Innovation

The war in Ukraine has underscored that technological interoperability and doctrinal innovation are vital to collective survivability.

For Romania, three lessons are essential:

- **Digital interoperability:** Romania must transition from legacy, conventional infrastructures to distributed C2 architectures, integrating secure tactical clouds and AI algorithms. By comparison, the Baltic states are already

far advanced in society-wide digitalisation, whereas Poland has invested in robust infrastructures that are deeply interoperable with US systems.

- **Accelerated innovation:** Romania should leverage its status as host of the European Cybersecurity Competence Centre (ECCC) to evolve into a regional hub of military technological innovation. It entails not merely adoption for defence, but the development of indigenous, sovereign solutions – from uncrewed systems (UAS/drones) and advanced software to secure-by-design cyber infrastructures – anchored in an agile, dual-use innovation ecosystem.
- **Societal resilience:** The Baltic states offer the benchmark of Total Defence, whereby society in its entirety participates in national defence. Romania requires a whole-of-society strategy in which citizens, the private sector, and civil institutions are integrated into the resilience architecture.

Thus, Romania can transcend its status as a “*vulnerable node*” and become an innovative, resilient pillar on the Eastern Flank, contributing to the transformation of NATO into a multi-domain, adaptive, and anticipatory alliance.

CONCLUSIONS AND RECOMMENDATIONS

The analysis has demonstrated that emerging technologies are not mere power multipliers but structural determinants of resilience and operational effectiveness. The five-dimension analytical framework – command and control, intelligence and situational awareness, decision speed, operational agility, and systemic resilience – has enabled a comprehensive appraisal of how Romania, relative to Poland and the Baltic states, is positioned within the Eastern Flank’s security architecture.

The findings confirm that Romania plays a pivot role in the Black Sea, yet structural vulnerabilities persist in C2, logistics infrastructure, and cyber resilience. At the same time, opportunities stemming from integration into NATO and EU initiatives, as well as Romania’s status as host of the European Cybersecurity Competence Centre can convert these vulnerabilities into comparative advantages.

From a theoretical standpoint, the study contributes to consolidating the literature on the *Revolution in Military Affairs (RMA)*, showing that the transition toward a multi-domain, digitalised environment is not merely aspirational but an empirically validated reality, as evidenced by the Ukrainian conflict. On the epistemological plane, the article supports the claim that the informational-cognitive paradigm is becoming the centre of gravity of contemporary warfare, progressively displacing the industrial paradigm premised on mass and volume.

The results thus confirm recent trends in strategic theory and complement them with an applied perspective tailored to Romania and the Eastern Flank.

Building on these conclusions, the following strategic directions should guide the consolidation of Romania's security profile:

- Investments in cyber resilience. Develop distributed, redundant infrastructures capable of withstanding hybrid attacks and ensuring the continuity of critical functions during crises.
- Strengthening decentralised logistics. Implement modular, flexible support models – inspired by Ukraine's experience – to enable the rapid reconfiguration of logistics flows in contested environments.
- Technology partnerships. Leverage Romania's position within NATO and the EU to build industrial-technological alliances focused on uncrewed systems (UAS/drones), artificial intelligence, and secure communications infrastructures.
- Cultivating a culture of military innovation. Stimulate doctrinal experimentation and rapid institutional learning by establishing operational laboratories and integrating the academic and private sectors into the defence ecosystem.
- Institutionalising a whole-of-society strategy. Adapt the Baltic Total-Defence model to Romanian specificities by engaging civil society and the private sector in ensuring national resilience and continuity.

Taken together, the study confirms that strategic success on NATO's Eastern Flank hinges on member states' ability to integrate emerging technologies coherently, multidimensionally, and anticipatorily. For Romania, it implies overcoming structural vulnerabilities through resilience investment, doctrinal innovation, and technology partnerships, thereby reinforcing not only national security but also the collective credibility of the Alliance. In an era marked by strategic volatility and technological acceleration, adaptability will remain the fundamental criterion of survivability and operational effectiveness.

BIBLIOGRAPHICAL REFERENCES:

1. Alberts, D.S., Garstka, J.J., Stein, F.P. (1999). *Network centric warfare: Developing and leveraging information superiority*. Washington, DC: CCRP Publication Series.
2. Barros, G. (2023). *Ukrainian military innovation: Tactical and technological lessons*. Washington, DC: Institute for the Study of War.
3. Biddle, S., Friedman, J.A. (2022). *The battle of Donbas and the future of conventional warfare*, in *Survival*, 64(4), pp. 7-30, <https://doi.org/10.1080/00396338.2022.2090705>, retrieved on 22 August 2025.

4. Galeotti, M. (2022). *The weaponisation of everything: A field guide to the new way of war*. New Haven, CT: Yale University Press.
5. Horowitz, M.C. (2018). *Artificial intelligence, international competition, and the balance of power*, in *Texas National Security Review*, 1(3), pp. 36-57, <https://tnsr.org/2018/02/artificial-intelligence-international-competition-and-the-balance-of-power/>, retrieved on 30 September 2025.
6. Kofman, M., Lee, R. (2022). *Preliminary lessons in conventional warfighting from Russia's invasion of Ukraine: February-July 2022*. Arlington, VA: CAN, <https://www.cna.org>, retrieved on 30 September 2025.
7. Kofman, M., Lee, R. (2023). *The evolving character of war: Ukraine and the future of military innovation*. Washington, DC: Center for Strategic and International Studies, <https://www.csis.org>, retrieved on 30 September 2025.
8. Krepinevich, A.F. (1992). *The military-technical revolution: A preliminary assessment*. Washington, DC: Center for Strategic and Budgetary Assessments.
9. Mareš, M. (2022). *Hybrid threats in the context of the war in Ukraine*. *Vojenské rozhledy*, 31(4), pp. 5-19, <https://doi.org/10.3849/2336-2995.31.2022.04.005>, retrieved on 22 August 2025.
10. Murray, W., Knox, M. (2001). *The dynamics of military revolution, 1300-2050*. Cambridge: Cambridge University Press.
11. NATO (2021). *NATO warfighting capstone concept*. Norfolk, VA: Allied Command Transformation, <https://www.act.nato.int>, retrieved on 30 September 2025.
12. NATO (2022). *Strategic concept*. Madrid: NATO Summit, <https://www.nato.int>, retrieved on 30 September 2025.
13. Radin, A. (2023). *Technological resilience in modern conflict: Case studies from Ukraine*. Santa Monica, CA: RAND Corporation, <https://www.rand.org>, retrieved on 30 September 2025.
14. Reznikova, O. (2022). *National resilience and technological innovation during wartime*, in *Ukrainian Journal of Security Studies*, 8(3), pp. 45-63.
15. Ti, K., Kinsey, C. (2023). *Adaptive logistics in contested environments: Lessons from Ukraine*, in *Journal of Military Logistics*, 14(1), pp. 22-36.
16. Watling, J., Reynolds, N. (2022). *The Russian way of war: Lessons from Ukraine*. London: Royal United Services Institute, <https://rusi.org>, retrieved on 30 September 2025.

IMPLICATIONS OF HYBRID WARFARE ACTIVITIES ON THE MULTI-DOMAIN OPERATIONS OF NAVAL FORCES IN THE BLACK SEA

Navy Captain (Ret.) Professor Ion CHIORCEA

"Mircea cel Bătrân" Naval Academy, Constanța

Lieutenant Commander Andrei PAVĂL, Doctoral Student

"Carol I" National Defence University, Bucharest

DOI: 10.55535/RMT.2025.3.18

In a context marked by the strategic competition between the North Atlantic Treaty Organization and the United States of America, on the one hand, and the Russian Federation, on the other hand, the analysis begins with the definition of doctrinally recognized operational domains: land, air, maritime, space, and cyber, to which are added the cognitive/information dimension and the civil cooperation dimension. The applied methodology relies on a multi-criteria comparative analysis of the implications of hybrid warfare activities on each domain, by identifying five relevant types of threats. The expected results are aimed at providing a doctrinal basis for establishing multi-domain formations within NATO and their applicability at the national level, with an emphasis on the specific features of the Black Sea operational environment. The novelty element lies in the systematic correlation of hybrid warfare threats with the integration capacity of multi-domain formations, offering recommendations for adapting naval forces towards the 2030 horizon.

Keywords: hybrid warfare; multi-domain operations; naval forces; Black Sea; multi-domain formations;

INTRODUCTION

The current international security environment is characterized by heightened strategic competition, in which great powers vie for supremacy across all dimensions of the operational environment. Recent conflicts, from the Russian Federation's aggression against Ukraine to escalations in the Middle East, have demonstrated that the boundaries between peace, crisis, and war are increasingly blurred, and military operations can no longer be conceived solely through the lens of a single operational domain. In this context, the concept of multi-domain operations (MDO) has emerged as a doctrinal response to the complexity of the strategic environment, being institutionalized by the US Armed Forces and gradually adopted by the North Atlantic Treaty Organization (NATO) as a foundation for future campaign planning.

At the US level, initiatives such as JADC2 (Joint All-Domain Command and Control) and "*project overmatch*" constitute the pillars of military transformation. JADC2 aims to create an integrated architecture capable of connecting sensors and effectors across all domains into a single network, in order to deliver rapid decision-making in an environment saturated with electromagnetic warfare and cyberattacks. In parallel, the US Navy seeks, through "*project overmatch*", to integrate artificial intelligence and autonomous systems into dispersed naval operations, in order to maintain the advantage in an increasingly contested maritime domain (Hoehn, 2021). Both programs confirm the strategic direction toward the year 2030¹ (Cucinschi, 2024), a direction doctrinally reinforced through "*FM 3-0 Operations*" (2025), which explicitly states that "*all operations are multi-domain operations*" (Headquarters, Department of the Army, 2025, p. 17), applicable at all echelons and in all strategic contexts: peace, crisis, and war (ib., pp. 16-17).

¹ The United States' objective was defined in "*TRADOC Pamphlet 525-3-1*" (2018), which refers to an army capable of multi-domain operations (MDO) by the year 2028 (US Army Training and Doctrine Command, 2018). Subsequently, "*FM 3-0 Operations*" (2022) explicitly referred to the 2030 timeframe under the "*Army 2030*" vision, while the updated edition, "*FM 3-0 Operations*" (2025), no longer sets a calendar year but doctrinally reinforces the principle that "*all operations are multi-domain operations*" (Headquarters, Department of the Army, 2025). Within NATO doctrine, the concept of MDO was officially institutionalized through "*AJP-3 Allied Joint Doctrine for the Conduct of Operations*" (2019) and later expanded by Allied Command Transformation (2025), though without specifying a precise year for implementation. In this study, the year 2030 is employed as an analytical benchmark, inferred from the US objective and the presumed alignment of the Alliance as a whole with this strategic direction.

In parallel, NATO explicitly acknowledged the importance of multi-domain integration through *“AJP-3, Allied Joint Doctrine for the Conduct of Operations”* (2019), as well as within specialized conferences held under Allied Command Transformation (Allied Command Transformation, 2025). They institutionalize not only the classical domains: land, air, maritime, space, and cyber, but also emphasize the significance of the cognitive/information dimension and the civil cooperation dimension as indispensable functions for achieving operational superiority (North Atlantic Treaty Organization, 2019). Thus, the Allied framework confirms that the success of multi-domain operations depends on integrating military and civilian resources, shaping perceptions, and strengthening social resilience.

Nevertheless, the application of MDO in geographically constrained and contested regions such as the Black Sea raises significant challenges. The Pontic area is marked by the presence of the Russian Federation Navy (RFN), the militarization of the Crimean Peninsula, and the use of hybrid techniques and tactics (e.g., disinformation, cyberattacks, exploitation of civilian infrastructure, challenging the international legal regime etc.). At the same time, for NATO and the littoral states, the Black Sea holds a distinct strategic role by ensuring freedom of navigation, securing maritime energy infrastructure, and supporting vulnerable partners (Vdovychenko, Albu, Chitadze, 2024; Kohler, 2020). This dual relevance, vital for both Russia and NATO, creates the premises of a contested environment, where hybrid warfare activities become instruments for eroding cohesion and undermining freedom of navigation in the Black Sea.

Previous research has focused primarily on the doctrinal definition of MDO and on the development of technological capabilities required for its implementation. However, it remains unclear to what extent hybrid warfare activities can undermine multi-domain convergence in semi-enclosed theatres of operations such as the Black Sea. This gap is particularly relevant for Romania, a Black Sea littoral state which, through its NATO membership, follows the trajectory of implementing multi-domain formations (MDF) by the 2030 horizon. Nevertheless, structural vulnerabilities, such as insufficiently protected critical port infrastructure, dependence on civilian resources, and lack of strategic depth, raise questions regarding the pace and consistency of practically translating this objective into reality.

The purpose of this study is to critically examine the implications of hybrid warfare activities on each domain of MDO, with particular focus on the Black Sea operational environment and on the role of the Romanian Naval Forces.

The proposed methodology, a multi-criteria comparative analysis, enables the identification of five types of hybrid warfare threats for each domain/dimension and the assessment of their implications for the practical implementation of MDO through MDF. The results aim both to clarify vulnerabilities and to formulate doctrinally and operationally applicable recommendations designed to enhance the resilience of the naval forces and their interoperability with the Allies.

The novelty of this study originates from the systematic correlation of hybrid activities with the vulnerabilities of MDO domains and their translation into a forward-looking framework for the implementation of naval MDF in the Black Sea. This approach does not remain confined to a theoretical description but seeks to provide a comparative, future-oriented framework for Allied strategic planning in the Black Sea region. In this way, the study contributes to the specialized literature and delivers practical value for the Romanian Naval Forces, demonstrating that the success of implementing MDF towards 2030 depends not only on technological modernization and doctrinal adaptation but also on the ability to effectively counter hybrid warfare activities that define the current security environment.

This analysis is based on the hypothesis that hybrid activities generate asymmetric effects across different domains, being particularly pronounced in the maritime domain while maintaining close interdependence with the other operational domains. The central research question guiding this study is: *How do hybrid warfare activities affect the capacity of the naval forces in the Black Sea to implement MDO by the 2030 horizon, and what doctrinal, technological, and organizational adaptations are required for multi-domain formations?* To answer this question, the research seeks to define the domains of MDO and tailor them to the specifics of the Black Sea region, to identify and analyse five relevant hybrid warfare activities for each domain, to assess their implications through a multi-criteria comparative analysis, and to examine their impact on the Romanian Naval Forces and NATO. Finally, the study proposes doctrinally and operationally applicable recommendations intended to strengthen resilience and interoperability within MDF. The structure of the paper follows a logical progression, from the conceptual analysis of MDO domains and the identification of relevant hybrid warfare threats, to the application of a multi-criteria comparative method and the extraction of conclusions and recommendations for the doctrinal and operational adaptation of the naval forces.

STATE OF THE ART IN THE FIELD

The specialized literature on hybrid warfare is extensive, reflecting the constant concern of both the academic and doctrinal communities with the ambiguous and multidimensional nature of this type of conflict. Analyses emphasize that hybrid warfare entails a fluid combination of conventional and unconventional means, both military and non-military, to exploit the vulnerabilities of adversaries. Ferris (2012) shows that the phenomenon is not new, having historical roots in imperial conflicts, but has gained increased relevance in the 21st century. Batyuk (2017) highlights that the term was adopted by the United States of America as a conceptual tool to describe tactics of strategic coercion below the threshold of conventional conflict. Grier (2017) warns of the risk that “*hybridity*” may become a mere *buzzword*², losing analytical value, an idea echoed by Wither (2023), who criticizes the lack of conceptual clarity. In the same vein, Tagarev (2021) proposes new analytical frameworks for hybrid warfare threats, stressing the need for a systemic approach.

In the maritime domain, recent research confirms the adaptability of hybrid warfare and, implicitly, the activities associated with this type of conflict. Studies such as those by Schaub, Murphy and Hoffman (2017) or Mitrescu and Sokolov (2025) show that critical maritime infrastructure has become a primary target for hybrid warfare threats, while Stensrud and Østhagen (2024) describe the tactical application of Russian new-generation warfare in areas such as the Arctic and the Black Sea. These works confirm that hybrid warfare plays a central role in strategies of destabilization and in challenging the international order.

With regard to MDO, the literature remains at an early stage, being strongly influenced by US doctrine. The manuals – US Army Training and Doctrine Command (2018) and Headquarters, Department of the Army (2025) have established MDO as a new operational concept, defining the simultaneous integration of all domains to create relative advantages over adversaries. Complementarily, reports on JADC2 and “*project overmatch*” (Hoehn, 2021) indicate the technological direction of integrating sensors and effectors across all domains. At the NATO level, doctrine (North Atlantic Treaty Organization, 2019) and recent initiatives of Allied Command Transformation (2025) confirm the relevance of the multi-domain operations approach, though without specifying a clear implementation timeline. According to US doctrine, it is necessary to distinguish between MDO, defined as a doctrine that integrates all domains to create relative advantages, and MDF, conceived

² The term “*buzzword*” refers to a fashionable word or expression, frequently used in political, academic, or media discourse, risking the loss of its analytical meaning through overuse and ambiguity.

as organizational instruments through which this doctrine is put into practice, designed to penetrate and disintegrate adversary A2/AD (Anti-Access/Area Denial) systems and exploit the advantage and freedom of manoeuvre thus achieved (US Army Training and Doctrine Command, 2018, p. 5). Nevertheless, although MDF are theoretically presented as ideal solutions for the operationalization of MDO, their application in restricted, semi-enclosed, and contested maritime spaces such as the Black Sea raises questions regarding the feasibility and adaptability of this model to regional geopolitical and infrastructural realities.

Last but not least, at the academic level, Kohler (2020) highlights the necessity of integrating naval forces into the Joint Force Maritime Component Command in order to counter Russian influence in the Black Sea, while Vdovychenko, Albu and Chitadze (2024) analyse the region's security trilemma, defined by the interaction between Türkiye's own interests, the pro-western orientation of Ukraine and the allied Black Sea littoral states, and the Russian Federation's objective of maintaining its influence. Other contributions, such as Islam (2024) and Scutaru, Pavel (2025), expand the debate on regional cooperation and on the resilience of critical infrastructure.

A critical review of the specialized literature reveals a disproportion: the amount of work on hybrid warfare is abundant and diverse, with numerous case studies and conceptual approaches, while research on MDO, particularly with respect to the Black Sea region, remains anchored mainly in US doctrine and NATO's early attempts at adaptation. Moreover, causal analysis of how hybrid warfare activities directly influence the implementation of MDO is nearly absent. This gap justifies the present study, which proposes a systematic correlation between the two concepts and their contextualization for the Black Sea theatre of operations. In this regard, the need to examine hybrid warfare threats in the Pontic area, intensively studied and debated in the literature, becomes essential for understanding how they affect the applicability of MDO and, implicitly, MDF in the region. Furthermore, given that state actors such as the United States of America are approaching the final phase of the timeline assumed for the implementation of these MDF, shaping the operational environment prior to implementation is imperative in order to support both doctrinal adaptation and the practical preparation of the Romanian Naval Forces and NATO in the Black Sea.

METHODOLOGY

The methodology of this article is designed to provide a systematic analytical framework through which the central objective can be achieved: identifying the implications of hybrid warfare activities on MDO and on the capacity of the naval forces in the Black Sea to implement multi-domain formations by the 2030 horizon. This methodological approach is directly aligned with the research question and the previously stated objectives, offering the instruments through which the analysis can highlight how these implications influence the practical translation of MDO and MDF doctrines in the Black Sea region. In military research, methodology is not merely a set of technical procedures but represents the foundation through which data are collected, interpreted, and transformed into doctrinally applicable results (Creswell, Creswell, 2018).

The main method employed is a multi-criteria comparative analysis of the implications of hybrid warfare activities on each domain/dimension of MDO. The selection of this method is justified by the complex and interdependent nature of operational domains, where threats cannot be analysed in isolation but only in relation to an integrated whole. The model is inspired by multi-criteria assessments applied in security studies, which enable the qualitative quantification of implications (Tagarev, 2021). Within this framework, the research identifies five hybrid warfare activities representative for each MDO domain, selected on the basis of specialized literature and NATO and US doctrinal documents, though not limited exclusively to these sources.

The data used derive from doctrinal documents, which provide the conceptual framework and the implementation timeline; from recent academic literature, which offers critical perspectives on hybrid warfare and MDO, as well as from regional case studies specific to the Black Sea, focused on the effects of hybrid tactics on maritime security. The processing of these data involves scoring the identified hybrid warfare activities, assessing their implications (intensity, probability, and relevance) on a scale from 1 to 5, and integrating them into a comparative matrix.

The selection of the 1-to-5 scale has a methodological foundation. According to Creswell and Creswell (2018), the use of a simple and standardized scale allows the integration of qualitative and quantitative data into a convergent mixed-methods approach. In this article, the value 1 corresponds to minor implications, where the hybrid activity has limited effects on the analysed domain, while the value 5 designates critical implications, capable of decisively affecting cohesion and multi-domain integration capacity. Intermediate values (2-4) reflect gradations

of intensity, probability, and relevance, calibrated on the basis of frequency and severity (impact) identified in the specialized literature and doctrinal documents. This scaling facilitates comparability across domains and transforms qualitative analysis into a predictive tool with applicability for operational planning (Creswell, Creswell).

The analysis is critically oriented, in the sense that it does not limit itself to reproducing doctrinal definitions but seeks to highlight the discrepancies between theory and practical applicability. For example, US Army Training and Doctrine Command (2018) clearly defines the distinction between MDO as doctrine and MDF as an organizational instrument, yet it remains unclear how these MDF can be adapted to semi-enclosed and contested spaces such as the Black Sea. For this reason, the research proposes correlating the implications of hybrid warfare activities with the vulnerabilities of each MDO domain, as an exercise in anticipatory modelling prior to the actual implementation of MDF.

Through this approach, the methodology contributes not only to validating the research question but also to establishing an analytical framework that can be replicated in other similar maritime regions. In addition, the results obtained will support the doctrinal adaptation of the Romanian Naval Forces and may provide a planning instrument oriented toward resilience and interoperability. The structure of the following chapters reflects this approach: first, the MDO domains will be defined with a particular focus on the Black Sea region. Then, each domain will be analysed in relation to the implications of hybrid warfare activities, based on the previously described method.

DOMAINS AND DIMENSIONS OF MULTI-DOMAIN OPERATIONS AND THEIR PARTICULARIZATION FOR THE BLACK SEA REGION

MDO represent one of the most significant doctrinal transformations of the 21st century, providing an integrated framework through which armed forces can achieve simultaneous superiority across all dimensions of modern conflict. Studying the dimensions of MDO is essential not only for understanding the mechanisms through which great powers project force, but also for identifying vulnerabilities that adversaries may exploit through hybrid warfare activities. States such as the USA have adopted the concept of multi-domain operations (MDO) as a reference doctrine and have initiated the development of multi-domain task forces (MDTF) as experimental structures, designed to penetrate and disintegrate A2/AD systems and to exploit the advantage and freedom of manoeuvre thus achieved.

They represent the precursors of multi-domain formations (MDF) currently under development, intended to ensure in the future the large-scale implementation of MDO and to consolidate an anticipatory approach to strategic competition (US Army Training and Doctrine Command, 2018). For the Black Sea context, the present analysis will refer exclusively to the concept of MDO and to MDF, given that MDTF remain experimental structures, developed at present only by the United States of America. In this context, the analysis of MDO begins with the definition of doctrinally recognized operational domains: land, air, maritime, space, and cyber, to which are added the cognitive/information dimension and the civil cooperation dimension. In contested and semi-enclosed regions such as the Black Sea, contextualizing the domains and dimensions of MDO becomes a critical condition for operationalizing the doctrine and for adapting the naval forces to NATO requirements and the characteristics of the current security environment.

Land Domain

It constitutes the fundamental dimension of warfare, as it encompasses control of physical space, force mobility, and support for operations in the other domains. Current US doctrine emphasizes that land manoeuvre does not occur in isolation but is permanently interconnected with effects generated in the air, maritime, space, and cyber domains (Headquarters, Department of the Army, 2025). This approach reflects the transformation of land operations from a traditional dimension into a vector of multi-domain integration.

Within MDO and MDF, the land domain acquires particular relevance through its role in penetrating and disintegrating A2/AD systems, thereby facilitating freedom of action for air, naval, and space forces (US Army Training and Doctrine Command, 2018). Thus, land forces no longer have an exclusively ground manoeuvre role but become an integral part of a system that generates simultaneous relative advantages across all domains.

Across the Black Sea region, the land domain has critical particularities: the territories of Romania and Bulgaria serve as strategic staging points for NATO force deployment, while road, rail, and force logistics infrastructure constitute an essential condition for supporting air and maritime operations. However, this infrastructure can become vulnerable to hybrid sabotage of transport routes and logistic facilities (Eckel, 2025), to the infiltration of proxy and paramilitary forces

supported externally (Beznosiuk, 2025), or to lawfare³ tactics that challenge troop deployments and generate strategic ambiguity (Bachmann, Mosquera, 2015). In parallel, the use of suicide drones and loitering munitions⁴ transforms the tactical battlefield into an environment saturated with asymmetric risks (Kunertova, 2023), while GNSS (Global Navigation Satellite System) jamming and spoofing⁵ can undermine the coordination and mobility of land forces (Schmidt, Radke, Camtepe, Foo, Ren, 2016). In addition, capabilities such as amphibious assault and special operations forces directly connect the land domain with the maritime and air domains, providing flexibility in countering these hybrid warfare activities and in supporting integrated multi-domain operations.

Air Domain

It represents one of the essential domains of power projection, providing rapid mobility, strategic surveillance, and precision strike capability. US doctrine defines airpower as an indispensable instrument for achieving superiority in modern conflict, emphasizing its interdependence with the other operational domains (US Air Force, 2021). By virtue of its flexible and global character, airpower enables decisive actions within short timeframes; however, it faces significant constraints in highly contested operational environments such as the Black Sea, dominated by A2/AD systems.

In the context of MDO, the air domain plays a central role in integrating reconnaissance, command, and strike systems, while simultaneously supporting land, naval, and space forces. MDF depend on aviation for penetrating A2/AD systems and for synchronizing effects across all domains (US Army Training and Doctrine Command, 2018). Thus, aviation is not merely a supporting vector but a critical link for the success of multi-domain operations.

In the Black Sea region, the air domain faces complex particularities: the presence of Russian S-400 air defence systems in Crimea restricts freedom of air manoeuvre, while GNSS jamming undermines navigation and coordination.

³ The term *lawfare* comes from the combination of law and warfare and involves the strategic use of legal instruments as a weapon of war, with the aim of limiting the opponent's freedom of action, challenging the legitimacy of troop deployment or creating strategic ambiguities. The concept is analysed in the international security literature as part of the spectrum of actions associated with hybrid warfare, being correlated with both the manipulation of the international legal framework and the exploitation of domestic regulations to achieve political-military objectives (Orde, 2016).

⁴ The term *loitering munition* designates a type of unmanned aerial weapon that combines the characteristics of a drone with those of a precision munition.

⁵ The term *spoofing* designates a computer attack technique through which false signals or data are generated, intended to imitate legitimate sources, with the aim of deceiving receiving systems.

The use of drones and loitering munitions has demonstrated the vulnerability of air bases and critical infrastructure (Kunertova, 2023; Plichta, 2025). In addition, electromagnetic warfare operations, cyberattacks against aviation infrastructure, and multi-vector saturation strikes put the resilience of air forces under pressure, creating significant risks for the air domain as part of MDO in the Black Sea region (Florida-Benítez, 2024; Dalsjö, Jonsson, Norberg, 2022).

Maritime Domain

Alongside the air domain, it is another vital domain for power projection and freedom of navigation, ensuring both control of sea lines of communication (SLOC) and protection of critical infrastructure. US naval doctrine emphasizes that maritime power integrates surface, submarine, and air-maritime actions, being indispensable for deterring adversaries and for ensuring access to contested areas (US Navy, 2025). From a multi-domain perspective, naval capabilities provide strategic mobility and support for land and air operations, while simultaneously depending on informational and cyber integration.

As part of MDO, the maritime domain plays a central role in penetrating A2/AD systems and in maintaining the freedom of manoeuvre of Allied forces. The role of MDF can be to generate simultaneous effects on the surface, underwater, and in the air domain, thereby supporting synchronization with land and air forces (US Army Training and Doctrine Command, 2018). Thus, the navy is not merely a force of presence and deterrence but a critical component of multi-domain integration.

Throughout the Black Sea area, the maritime domain is strongly influenced by the presence and militarization of the RFN, as well as by the location of critical infrastructure in close proximity to risk areas. Specific hybrid warfare activities include the sabotage of critical maritime infrastructure, the use of autonomous naval drones against ports and ships, AIS/GPS (Automatic Identification System/Global Positioning System) navigation system spoofing, the disruption of commercial traffic through the declaration of maritime areas as exercise zones, and the deliberate harassment of vessels through dangerous approach manoeuvres (Monaghan, Connolly, 2023, p. 23; Burlacu, Sandu, 2023; Zorri, Kessler, 2024; Gaber, 2024; Sabanadze, Dalay, 2025; Godzimirski, Mitrescu, 2025). These tactics increase the risk of escalation and undermine regional maritime security, affecting the capacity of the maritime domain to be integrated into multi-domain operations.

Space Domain

It has become a central pillar of modern operations, providing secure communications, global surveillance, and support for navigation and the precise guidance of modern munitions. US Space Force (2025) defines space as a distinct operational environment, in which the control and protection of satellite infrastructure are essential for the conduct of any military campaign. In the current logic of warfare, satellites no longer serve solely as tools for information gathering but have become direct operational instruments within the multi-domain architecture.

Embedded in MDO, the space domain is critical for simultaneously connecting all domains, from land and maritime to air and cyber. MDF rely on satellite services for action coordination and for ensuring the resilience of command and control (C2) systems in highly contested operational environments (US Army Training and Doctrine Command, *ib.*). Space, by its global nature, provides freedom of manoeuvre and informational superiority but at the same time becomes a hybrid confrontation arena where strategic competition is intense.

Across the Black Sea region, where the operational environment is defined by the presence of A2/AD systems and the interdependence of critical infrastructure, space assumes a decisive role. Hybrid warfare activities manifest through jamming and spoofing of satellite communications (Peled, Aizikovich, Habler, Elovici, Shabtai, 2023), cyberattacks against satellite systems (Peled, Aizikovich, Habler, Elovici, Shabtai, 2023), use of kinetic and non-kinetic anti-satellite technologies (Grossfeld, 2024), hostile proximity manoeuvres against Allied satellites (Egeli, 2021), and exploitation of informational ambiguity in space communications to generate strategic confusion (Höyhty, Uusipaavalniemi, 2023). These practices undermine confidence in space advantage and place pressure on the ability of the naval forces and NATO to safely integrate space services as part of the space domain in MDO in the Black Sea region.

Cyber Domain

This domain has become indispensable in modern conflict, being doctrinally recognized as a distinct operational environment in which activities of defence, attack, and information exploitation are conducted. NATO has both defined and institutionalized the role of the cyber domain, emphasizing network security and the protection of information flows as essential elements for the success of any joint operation (North Atlantic Treaty Organization, 2019). In US doctrine, operations in cyberspace complement actions in the land, air, maritime, and space environments, ensuring rapid interconnection and resilience, particularly of C2 systems.

In the framework of MDO, the cyber domain serves as the connective tissue linking all other dimensions. MDF rely on the security of digital communications to coordinate actions simultaneously but remain exposed to persistent attacks aimed at degrading networks and compromising informational advantages (US Army Training and Doctrine Command, ib.). Ensuring freedom of action in cyberspace constitutes a decisive factor for maintaining operational tempo and for strengthening interoperability among Allied forces and, implicitly, within multi-domain formations.

In the Black Sea region, hybrid warfare activities targeting the cyber domain are multiple and recurrent. Ransomware⁶ attacks have already struck critical infrastructure, disrupting the functioning of logistics and transport networks (Schwarz, Marx, Federrath, 2021). Stealth infiltrations⁷ into naval networks can undermine the detection and reaction capacity of Allied forces (Todorov, 2024), while AI (Artificial Intelligence) – and IoT (Internet of Things)-based automated systems can be manipulated to generate operational confusion (Fenton, 2024). In parallel, disinformation campaigns amplified through cyber channels erode public trust and political cohesion (Usewicz, Keplin, 2023), while DDoS (Distributed Denial of Service) attacks can paralyze C2 centres, limiting multi-domain coordination. These practices undermine regional security and pose major challenges for integrating the naval forces and NATO into a coherent operational architecture in the Black Sea region.

Cognitive/Information Dimension

This dimension is increasingly prominent in the analysis of modern conflicts, reflecting the interdependence between the information environment, decision-making processes, and collective perceptions. While US doctrine does not define it as a standalone domain of MDO, NATO treats it as a connected dimension, indispensable for achieving and maintaining operational advantage, especially in the current context in which Allied states in Eastern Europe face growing challenges in this spectrum. This perspective underscores that victories are not achieved solely through physical manoeuvres but also through the ability to influence the adversary's will and the resilience of one's own societies.

⁶ *Ransomware* refers to a type of cyber attack in which an organization's data is encrypted, and access to it is conditional on paying a sum of money to the attacker.

⁷ *Stealth infiltration* refers to the discreet and persistent penetration of a computer system, through techniques designed to avoid detection and maintain long-term access.

Regarding MDO, the cognitive dimension supports the integration of the other domains by strengthening legitimacy and preserving cohesion. MDF depend on informational resilience and on the ability to counter adversarial campaigns aimed at the will to fight, trust in institutions, and political stability. Unlike the classical domains: land, air, maritime, space, and cyber, the cognitive/information dimension operates primarily on perceptions, collective memory, and decision-making psychology, which grants it a distinct value in the logic of hybrid confrontations.

With respect to the Black Sea region, this dimension is heavily exploited by the Russian Federation and other actors through hybrid campaigns that include: shaping public discourse via disinformation and propaganda (Deppe, Schaal, 2024), coordinated operations in the digital space combining mass media, social networks, and emerging technologies (Deppe, 2023), algorithmic manipulation and the use of bot networks to amplify false messages (Gombar, 2025), dissemination of strategically targeted fake news to erode trust in institutions (Bârgăoanu, Godzimirski, Ioniță, 2020), and foreign information manipulation and interference (FIMI) campaigns designed to undermine democratic processes and NATO cohesion (Proto, Lamoso-González, García, 2025). These practices create vulnerabilities that are difficult to counter, with direct implications for the implementation of MDO and for regional resilience in the Black Sea.

Civil Cooperation Dimension

The relationship between the military and the civilian environment is a fundamental element of national resilience and of collective defence capacity. NATO doctrine underscores the importance of coordination between military authorities and civilian structures in order to support the conduct of joint operations and to ensure the continuity of essential societal functions (North Atlantic Treaty Organization, 2025). Unlike the doctrinal domains recognized by the US Army Training and Doctrine Command (2018): land, air, maritime, space, and cyber, the relationship with the civilian environment is not defined as a standalone domain of MDO, but is treated instead as a connected dimension, indispensable for implementing MDO in contested environments.

Under MDO architecture, this dimension plays the role of integrating civilian resources and ensuring logistic, energy, and social support for the conduct of operations. Multi-Domain Formations (MDF) rely not only on interoperability among Allied armed forces but also on the ability to employ dual-use civilian infrastructure, to cooperate with national and local authorities, and to sustain public support.

The vulnerability of these relations makes the civil cooperation dimension a primary target of hybrid warfare activities, with the potential to undermine cohesion and erode regional resilience.

Across the Black Sea region, these vulnerabilities are amplified by the strategic context and the proximity of the conflict in Ukraine. Hybrid warfare activities have materialized through the sabotage of critical civilian infrastructure with military relevance (Soldi et al., 2023), cyberattacks against public utility infrastructure with impact on the population and logistics (Fenton, 2024), the exploitation of refugee flows as a tool of political pressure and destabilization (Łubiński, 2022), disinformation campaigns undermining public support for defence, and attacks on dual-use civilian logistics such as ports or transport companies. All these elements highlight that the civil cooperation dimension is vulnerable to hybrid warfare activities, and that protecting this dimension becomes an essential condition for the success of MDO and for maintaining NATO cohesion in the Black Sea region.

HYBRID WARFARE ACTIVITIES IN THE BLACK SEA REGION AND THEIR IMPLICATIONS FOR MDO/MDF

The diversity of hybrid warfare activities requires a careful selection of those that can directly influence the implementation of the MDO doctrine and the establishment of MDF in the Black Sea. The brief description of the domains and dimensions of MDO has shown that they were not delineated by chance, each contributing to the integration and coherence of the operational whole. This section identifies the hybrid warfare threats relevant to each domain/dimension, with implications for the capacity of the naval forces in the Black Sea to implement MDO concepts and, implicitly, MDF, in a strategic environment that is both versatile and contested by the region's main state and non-state actors.

Land Domain (LD)

- *LD1: The use of suicide drones and loitering munitions that affect land mobility and the coastal support of multi-domain operations;*
- *LD2: The sabotage of critical land infrastructure that limits strategic mobility and the logistic support of harbour areas;*
- *LD3: Proxy force operations that generate strategic ambiguity and undermine land security in maritime access areas;*
- *LD4: The disruption of navigation through GNSS jamming that restricts land mobility and the logistic connection with maritime operations;*

- *LD5: The exploitation of international and national legislation aimed at blocking troop deployments and delegitimizing military actions.*

Air Domain (AD)

- *AD1: GNSS jamming and spoofing that affect air navigation and reduce multi-domain synchronization in regional operations;*
- *AD2: Kamikaze drone and loitering munition attacks that saturate defences and diminish the operational capacity of air bases;*
- *AD3: Electromagnetic warfare operations and aerial decoys that degrade radars and reduce the effectiveness of integrated air defence;*
- *AD4: Cyberattacks against air infrastructure that disrupt operations and slow the tempo of multi-domain integration;*
- *AD5: Multi-vector saturation strikes that overwhelm air defence and reduce the resilience of national and Allied air capabilities.*

Maritime Domain (MD)

- *MD1: The sabotage of critical maritime infrastructure that destabilizes logistic and energy chains in the Black Sea;*
- *MD2: The use of unmanned surface vessels (USVs) conducting hard-to-detect offensive attacks against maritime targets;*
- *MD3: AIS and GPS spoofing that distorts ship positioning and creates erroneous perceptions in the maritime domain;*
- *MD4: The obstruction of freedom of navigation by restricting maritime areas declared as naval exercises, with effects on maritime commercial traffic;*
- *MD5: Naval harassment through dangerous manoeuvres and aggressive approaches that intimidate and destabilize safe navigation.*

Space Domain (SD)

- *SD1: Space-based jamming and spoofing that degrade military communications and compromise the synchronization of multi-domain operations;*
- *SD2: Cyberattacks against civilian and military communication satellites that affect Allied operational-strategic responsiveness;*
- *SD3: Kinetic and non-kinetic attacks against satellites that degrade satellite services and disrupt the functioning of the space domain;*
- *SD4: Aggressive proximity manoeuvres in space that compromise satellite integrity and interrupt informational communication networks;*

- *SD5: The exploitation of disinformation and ambiguity regarding space activities that induce uncertainty and erode operational credibility.*

Cyber Domain (CD)

- *CD1: Ransomware attacks against critical infrastructure that block logistic services and disrupt the interoperability of multi-domain operations;*
- *CD2: Disinformation campaigns in cyberspace that erode trust in headquarters and destabilize the information environment;*
- *CD3: Stealth and persistent infiltrations into naval networks that sabotage and hinder Allied detection and response;*
- *CD4: The compromise of AI- and IoT-based automated systems that can be manipulated to generate confusion in the operational domain;*
- *CD5: Coordinated DDoS attacks against command centres that block data transmission to multi-domain formations.*

Cognitive/Information Dimension (CID)

- *CID1: Shaping public discourse through disinformation and propaganda that weaken social cohesion and collective resilience;*
- *CID2: Online information campaigns using mass media, social networks, and emerging technologies to manipulate opinions and behaviours;*
- *CID3: Algorithmic manipulation and bot networks that amplify false messages and generate public opinion polarization;*
- *CID4: Strategically targeted fake news that erodes trust in institutions and undermines rational decision-making processes;*
- *CID5: Foreign information manipulation campaigns that undermine trust in governments and international organizations, affecting the cohesion of alliances and strategic partnerships.*

Civil Cooperation Dimension (CCD)

- *CCD1: The sabotage of civilian infrastructure with military relevance, which limits logistic support and reduces the resilience of multi-domain operations;*
- *CCD2: Cyberattacks against public infrastructure that cause major disruptions and affect the support of military operations;*
- *CCD3: The exploitation of refugee flows and forced migration as instruments of political pressure and social destabilization;*
- *CCD4: Disinformation campaigns that manipulate public perceptions and reduce civilian support for collective defence initiatives;*

- *CCD5: Attacks on dual-use civilian logistics that affect infrastructure essential both for commercial flows and for military support.*

MULTI-CRITERIA COMPARATIVE ANALYSIS OF THE IMPLICATIONS OF HYBRID WARFARE ACTIVITIES ON MDO AND MDF IN THE BLACK SEA REGION

The application of the methodology involves transforming the identified threats into comparative assessment instruments, in order to highlight how they affect multi-domain operations and the capacity of MDF to be constituted and to operate in the Black Sea region. Each domain has been analysed in relation to five characteristic threats, synthesized into short versions to facilitate their integration into a common analytical framework. The domains have been assessed based on three criteria: intensity (I), probability (P), and relevance (R) for MDF, each with values ranging from 1 to 5. The resulting scores do not represent mere numerical values but rather the outcome of a critical interpretative process designed to capture the interaction and interdependence between vulnerabilities and multi-domain response options.

Table 1: Assessment of the implications of hybrid warfare activities on the land domain

Hybrid warfare activities – land domain	I	P	R	Total	Implications for the MDO of naval forces in the Black Sea
LD1: Use of drones and loitering munitions	5	4	5	14	Reduce coastal protection capacity and expose naval logistic support lines
LD2: Sabotage of critical land infrastructure	4	4	5	13	Delay replenishment and restrict the freedom of manoeuvre of naval support
LD3: Proxy force operations	3	5	4	12	Weaken Allied coordination and endanger land support lines for naval forces
LD4: Land-based GNSS jamming	4	4	4	12	Hinder land manoeuvres and reduce the efficiency of coordination with naval support
LD5: Exploitation of legislation	3	3	4	10	Delay military response and reduce the freedom of action of joint naval operations

Hybrid warfare activities – land domain	I	P	R	Total	Implications for the MDO of naval forces in the Black Sea
Average score for the land domain	12.2 / 15				

In *table 1*, the main hybrid warfare activities affecting the land domain are presented, with emphasis on the use of drones, the sabotage of logistic infrastructure, and the infiltration of proxy forces. The high scores indicate that the vulnerability of infrastructure and transport routes can restrict the freedom of manoeuvre of naval forces and undermine the capacity of MDF to sustain coastal operations and to operate effectively in the land support area adjacent to the littoral.

Table 2: Assessment of the implications of hybrid warfare activities on the air domain

Hybrid warfare activities – air domain	I	P	R	Total	Implications for the MDO of naval forces in the Black Sea
AD1: GNSS jamming and spoofing	4	4	5	13	Disrupt air missions and limit reconnaissance and fire support for naval forces
AD2: Kamikaze drone and loitering munition attacks	5	4	5	14	Weaken air support and reduce the freedom of manoeuvre of naval operations
AD3: Electromagnetic warfare operations	4	4	5	13	Undermine air defence and expose naval forces to coordinated strikes
AD4: Cyberattacks against air infrastructure	4	3	4	11	Delay air support and affect the courses of action of naval forces
AD5: Multi-vector saturation strikes	5	3	5	13	Exhaust air defence and leave naval forces exposed to successive attacks
Average score for the air domain	12.8 / 15				

In *table 2*, the main hybrid warfare activities affecting the air domain are presented, among which GNSS jamming and spoofing, kamikaze drone attacks, and multi-vector strikes register the highest scores. These activities can disrupt air

Implications of Hybrid Warfare Activities on the Multi-Domain Operations
of Naval Forces in the Black Sea

missions, limit ISR (Intelligence, Surveillance and Reconnaissance) support, and reduce air defence protection, critical aspects for covering naval forces and for their integration into MDO in the Black Sea.

Table 3: Assessment of the implications of hybrid warfare activities on the maritime domain

Hybrid warfare activities – maritime domain	I	P	R	Total	Implications for the MDO of naval forces in the Black Sea
MD1: Sabotage of critical infrastructure	5	4	5	14	Disrupt essential energy and logistic flows supporting naval operations
MD2: Use of unmanned surface vessels	5	4	5	14	Threaten ship security and reduce freedom of navigation in coastal areas
MD3: AIS and GPS spoofing	4	4	5	13	Induce navigation errors, simulate illegal entries into TTW (territorial waters), and increase the risk of maritime incidents
MD4: Restriction of freedom of navigation	4	4	5	13	Limit freedom of navigation and reduce maritime mobility of Allied forces in the region
MD5: Naval harassment through dangerous manoeuvres	4	4	5	13	Increase the risk of collisions, diplomatic incidents, and undermine the security of Allied naval and maritime operations
Average score for the maritime domain	13.4 / 15				

In *table 3*, the main hybrid warfare activities affecting the maritime domain are presented, with high values assigned to the sabotage of critical maritime infrastructure and naval drone attacks. Other activities, such as AIS/GPS spoofing, restrictions on freedom of navigation, and naval harassment, highlight the vulnerability of freedom of navigation and the security of maritime operations in the Black Sea, particularly in the current context of the Russia-Ukraine conflict, when the presence of Allied naval forces is largely limited to maritime patrol aircraft missions.

Table 4: Assessment of the implications of hybrid warfare activities on the space domain

Hybrid warfare activities – space domain	I	P	R	Total	Implications for the MDO of naval forces in the Black Sea
SD1: Space-based jamming and spoofing	4	4	5	13	Disrupt navigation and reduce C2 coherence between naval and Allied components
SD2: Satellite cyberattacks	4	3	5	12	Weaken naval communications and delay synchronization of multi-domain operations
SD3: Attacks against satellites	5	2	5	12	Reduce GPS accuracy and limit the informational support of naval forces
SD4: Aggressive proximity manoeuvres in space	4	3	4	11	Reduce the reliability of satellite communications and affect naval operational coordination
SD5: Disinformation and ambiguity regarding space activities	3	4	4	11	Delay decision-making and reduce the operational cohesion of naval forces.
Average score for the space domain	11.8 / 15				

In *table 4*, the main hybrid warfare activities affecting the space domain are presented, among which jamming and spoofing, cyberattacks, and proximity manoeuvres register significant scores. These activities can affect satellite communications, navigation, and the synchronization of multi-domain operations, particularly in the maritime domain, where satellite services are essential for precise positioning and for the guidance of munitions trajectories during enemy engagement.

Implications of Hybrid Warfare Activities on the Multi-Domain Operations
of Naval Forces in the Black Sea

Table 5: Assessment of the implications of hybrid warfare activities on the cyber domain

Hybrid warfare activities – cyber domain	I	P	R	Total	Implications for the MDO of naval forces in the Black Sea
CD1: Ransomware attacks	4	4	5	13	Hinder logistic chains and reduce the reaction speed of naval forces
CD2: Disinformation campaigns in cyberspace	3	4	4	11	Undermine trust in C2 and reduce the operational cohesion of naval forces
CD3: Cyber infiltrations	4	4	5	13	Compromise information security and limit the effectiveness of joint naval defence
CD4: Compromise of automated systems	3	4	4	11	Disrupt digital architectures and reduce the predictability of multi-domain naval operations
CD5: DDoS attacks	4	4	5	13	Paralyze C2 flows and delay the reaction of naval forces
Average score for the cyber domain	12.2 / 15				

In *table 5*, the main hybrid warfare activities affecting the cyber domain are presented, with emphasis on ransomware attacks, persistent infiltrations, and DDoS attacks. These activities can compromise information security, disrupt C2 flows, and affect naval coordination in multi-domain operations, thereby reducing the reaction speed and resilience of MDF of the naval forces in the Black Sea.

Table 6: Assessment of the implications of hybrid warfare activities on the cognitive/information dimension

Hybrid warfare activities – cognitive/information dimension	I	P	R	Total	Implications for the MDO of naval forces in the Black Sea
CID1: Disinformation and propaganda	3	5	4	12	Erode public support and reduce the legitimacy of naval multi-domain actions

Hybrid warfare activities – cognitive/information dimension	I	P	R	Total	Implications for the MDO of naval forces in the Black Sea
CID2: Manipulative information campaigns	3	4	4	11	Distort collective perceptions and reduce public backing for joint naval operations
CID3: Manipulation through algorithms and bot networks	3	4	4	11	Undermine internal cohesion and reduce political support for implementing MDO in the Black Sea region
CID4: Strategically targeted fake news	3	4	4	11	Weaken trust in institutions and reduce public support for multi-domain operations
CID5: Foreign manipulation campaigns	4	3	5	12	Reduce Allied cohesion and weaken international support for establishing naval MDF in the Black Sea
Average score for the cognitive/information dimension	11.4 / 15				

In *table 6*, the main hybrid warfare activities affecting the cognitive and information dimension are presented, such as disinformation, manipulation through algorithms and bot networks, and strategically targeted fake news. These activities can erode social cohesion, trust in institutions, and public support for multi-domain operations, with an indirect impact on the legitimacy of Allied naval presence and on the political support for the establishment and implementation of MDF in the Black Sea region.

Table 7: Assessment of the implications of hybrid warfare activities on the civil cooperation dimension

Hybrid warfare activities – civil cooperation dimension	I	P	R	Total	Implications for the MDO of naval forces in the Black Sea
CCD1: Sabotage of civilian infrastructure with military relevance	5	4	5	14	Disrupt replenishment and reduce the resilience of support for multi-domain operations in the Black Sea

Implications of Hybrid Warfare Activities on the Multi-Domain Operations
of Naval Forces in the Black Sea

Hybrid warfare activities – civil cooperation dimension	I	P	R	Total	Implications for the MDO of naval forces in the Black Sea
CCD2: Cyberattacks against civilian infrastructure	4	4	4	12	Delay naval logistic support and affect the continuity of MDF operations in the region
CCD3: Exploitation of refugee flows and forced migration	3	4	3	10	Overstretch state resources and reduce the capacity to support MDF
CCD4: Disinformation campaigns	3	4	4	11	Reduce public acceptance of MDO implementation and delegitimize naval operations in the region
CCD5: Attacks on dual-use civilian logistics	4	4	5	13	Delay naval replenishment and limit the resilience of operational support in the Black Sea
Average score for the civil cooperation dimension	12.0 / 15				

In *table 7*, the main hybrid warfare activities affecting the civil cooperation dimension are presented, among which the sabotage of infrastructure, attacks on dual-use logistics, and disinformation campaigns register the highest scores. These activities can affect naval replenishment flows, the operating patterns of MDF, and public support for collective defence initiatives, underscoring the critical interdependence between the civilian and military sectors in the Black Sea region.

Table 8: Comparison of average scores across MDO domains and dimensions

Domain/Dimension	Average score (maximum 15)
LD - Land	12.2
AD - Air	12.8
MD - Maritime	13.4
SD - Space	11.8
CD - Cyber	12.2
CID - Cognitive/Information	11.4
CCD - Civil cooperation	12.0

In *table 8*, the average scores obtained for each analysed domain and dimension are synthesized. The results indicate that the maritime domain, in the Black Sea region, as part of multi-domain operations, faces the highest level of vulnerability to hybrid activities (13.4/15), followed by the air, land, and cyber domains, which directly support freedom of manoeuvre and the security of logistic flows. The space domain and the cognitive/information dimension, although recording lower values, generate significant cross-cutting effects, affecting multi-domain coordination and the legitimacy of Allied actions, particularly with regard to naval forces. At the same time, the civil cooperation dimension confirms the importance of critical and dual-use infrastructure, as well as social cohesion, for the operational resilience of MDF. This distribution of vulnerabilities constitutes the starting point for the integrated analysis of the results, in which the interdependence among domains becomes decisive for the success of multi-domain operations in the Black Sea region.

RESULTS

The application of the multi-criteria comparative analysis made it possible to transpose into a unified framework the thirty-five hybrid warfare activities identified for each domain/dimension as part of multi-domain operations. The results highlight significant differences between domains, as well as common trends with direct relevance for the capacity of the naval forces and NATO to constitute and operate MDF in the Black Sea region.

The highest level of vulnerability is found in the maritime domain (13.4/15), a fact explained by the concentration of threats against critical port infrastructure, the use of autonomous naval drones, and the restriction of freedom of navigation. This vulnerability is amplified by the context of the Russia-Ukraine conflict, in which the maritime domain directly supports land operations and provides the Russian Federation with a significant geographic advantage. The proximity of the Black Sea to Russian territory transforms this space into a strategic depth for Romania, at NATO's southeastern boarder, which intensifies the pressure on maritime security and freedom of navigation. The air domain ranks immediately after the maritime one, being exposed to GNSS jamming, kamikaze drone attacks, and multi-vector strikes, factors that reduce ISR support and the air defence protection necessary for naval operations. The land and cyber domains, located on the same risk tier (12.2/15), confirm the importance of logistics and information security: sabotage of infrastructure, persistent infiltrations, and ransomware attacks can block replenishment and disrupt C2 flows, diminishing the reaction capacity of MDF.

The civil cooperation dimension (12.0/15) underscores the critical interdependence between dual-use infrastructure and societal resilience, both indispensable for supporting the establishment and operation of MDF at the level of naval forces and for the public acceptance of Allied presence in the Black Sea region.

The lower scores recorded for the space domain (11.8/15) and the cognitive/information dimension (11.4/15) do not reflect a lack of relevance but rather their cross-cutting character. Jamming and attacks against satellites can simultaneously compromise navigation, communications, and cross-domain coordination, while information manipulation and the erosion of social cohesion can undermine legitimacy and the Allied decision-making capacity to sustain naval operations in the Black Sea. Overall, the results confirm the working hypothesis stated in the introduction, demonstrating that hybrid warfare activities produce asymmetric effects across domains, being particularly pronounced in the maritime domain, while at the same time manifesting through multiple interdependencies, with a cumulative effect on the implementation of multi-domain operations.

With regard to the limitations of the research, the analysis is based on data collected from open sources, which excludes both classified information and the lessons learned from NATO exercises in the Black Sea region or from the ongoing Russia-Ukraine conflict, as these cannot be fully documented through public sources. Secondly, the applied multi-criteria method provides a prospective perspective, useful for planning, but one that requires empirical validation through scenarios and wargaming exercises. Finally, the scores assigned to the implications of hybrid warfare activities may reflect a degree of subjectivity at the time of assessment, since they have been established on the basis of the available academic and doctrinal literature. These limitations do not diminish the value of the results but instead indicate future directions of research and justify the need for doctrinal and operational recommendations that address the research question set out in the introduction.

In this regard, the analysis provides a comparative framework that serves as the foundation for the conclusions and adaptation proposals formulated in the paper, oriented toward strengthening the capacity to implement the MDO doctrine and MDF in the Black Sea region.

CONCLUSIONS

The results obtained through the multi-criteria comparative analysis highlight that the maritime domain is the most vulnerable to hybrid warfare activities, followed by the air domain, while the land and cyber dimensions confirm the critical role of logistics and information security in supporting operations in the Black Sea region.

The space domain and the cognitive/information dimension, although recording lower scores, generate significant cross-cutting effects, while the civil cooperation dimension underscores the interdependence between critical infrastructure and social cohesion with operational resilience. These findings enable the formulation of an integrated response to the research question: *How do hybrid warfare activities affect the capacity of the naval forces in the Black Sea to implement MDO by the 2030 horizon, and what doctrinal, technological, and organizational adaptations are required for multi-domain formations?* Within this framework, the analysis has shown that hybrid warfare activities manifest in the logic of interdependence among domains/dimensions, with a cumulative effect on the implementation of the MDO doctrine and MDF in the Black Sea region.

The analysis has demonstrated that hybrid warfare activities employ a direct and disproportionate influence on the capacity to implement multi-domain operations in the Black Sea region. The maritime domain emerges as the most exposed, since freedom of navigation, the security of critical maritime infrastructure, and the protection of SLOC can be undermined by sabotage, naval drone attacks, or deliberate naval harassment. Vulnerabilities in the air domain amplify these risks by limiting ISR support and air defence protection, which in turn reduces the level of coordination and delays the reaction capacity of naval forces in the Black Sea.

At the same time, the land and cyber domains confirm that logistics and the security of information flows are essential elements for sustaining MDF. The sabotage of transport routes, proxy infiltrations, ransomware cyberattacks, or the compromise of C2 networks can block naval support and compromise the temporal coordination of naval operations. The space domain and the cognitive/information dimension, although scoring lower in the comparative analysis, generate cross-cutting effects with major impact: jamming and attacks against satellites can degrade navigation and communications, while information manipulation and the erosion of social cohesion undermine political legitimacy and public support. Equally, the civil cooperation dimension highlights the critical dependence of the naval forces on dual-use infrastructure and social resilience, without which freedom of manoeuvre and operational continuity cannot be ensured.

Therefore, hybrid warfare activities affect not only an isolated domain but the entire architecture of multi-domain operations, through a logic of interdependencies and cumulative effects. This reality demonstrates that the success of implementing MDF in the Black Sea region depends simultaneously on the protection of critical infrastructure, the safeguarding of information security, and the assurance of freedom of navigation.

To address the second part of the research question, it is necessary to identify doctrinal, technological, and organizational adaptations through which the naval forces can strengthen their resilience against hybrid warfare activities and ensure the effective implementation of MDF in the Black Sea region. Within this framework, the research has highlighted seven priority directions of action, with practical and forward-looking value, aimed at transforming theoretical results into concrete operational recommendations:

- the development of naval capabilities dedicated to the detection and neutralization of autonomous maritime drones, as well as to countering underwater sabotage, in order to protect critical infrastructure and SLOC;
- the development of naval capabilities equipped with automated short and medium-range air and missile defence systems, designed to intercept threats in the proximity of the maritime area and to transfer them to land-based long-range defence systems, with the aim of protecting MDF and, implicitly, national territory;
- the implementation of integrated protection mechanisms for dual-use infrastructure, such as harbours, energy networks, and transportation systems, through dedicated cooperation plans agreed at the interagency level;
- the adaptation of naval force training and MDF components for hybrid-type scenarios, by integrating them into training programs and into national and multinational exercises;
- the design of naval MDF as flexible and modular entities, capable of integrating land, naval, air, and cyber actions into a unified framework adapted to the specific security environment of the Black Sea;
- the integration of MDF into NATO's regional structures, with emphasis on the role of Romania and Bulgaria as littoral states and strategic staging points for operations in the Black Sea;
- the allocation of dedicated satellite support through the allocation of military satellites for naval MDF in the Black Sea, with redundancy mechanisms to ensure the continuous functioning of C2 systems and the sustained support of combat structures as integral components of MDF.

The recommendations formulated are aligned with the DOTMLPFI (Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities and Interoperability) framework and outline an initial, coherent adaptation plan for the naval forces and NATO in the Black Sea region. At the doctrinal level, MDO must be established as an operational-strategic foundation, while for MDF it is necessary to elaborate dedicated manuals and tactical procedures. From an organizational

perspective, priority should be given to the creation of flexible naval structures and their integration into NATO's regional architecture. In the field of training, scenarios of hybrid warfare activities must be systematically integrated into national and multinational exercises, with emphasis on ensuring freedom of navigation in the Black Sea. In terms of equipment, investments in counter-drone systems, anti-jamming capabilities, and redundant satellite assets are vital for safeguarding C2 resilience and freedom of navigation. Leadership requires strengthening through interdisciplinary training programs, and personnel must be selected and prepared to operate effectively at the fine intersection of MDO domains and dimensions. With regard to infrastructure, the modernization and maintenance of dual-use facilities such as harbours, energy nodes, and logistics hubs at high standards becomes essential for operational support. Finally, technological and procedural interoperability must be reinforced to efficiently integrate MDF into the Allied architecture. Thus, the success of implementing multi-domain formations in the Black Sea depends on an integrated transformation that combines doctrinal, organizational, technological, and social dimensions into a unified framework of resilience and adaptation.

BIBLIOGRAPHY:

1. Allied Command Transformation (24 August 2025). *Allied Command Transformation, Multi-Domain Operations Conferences*: https://www.act.nato.int/activities/multi-domain-operations/?utm_source=chatgpt.com, retrieved on 30 August 2025.
2. Bachmann, S.D., Mosquera, A.M. (2015). *Lawfare and hybrid warfare – how Russia is using the law as a weapon*. *The Military Law and the Law of War Review*, pp. 45-58, <https://journals.sas.ac.uk/amicus/article/view/2433/2395>, retrieved on 30 August 2025.
3. Batyuk, V. (3 September 2017). *The US concept and practice of hybrid warfare*. *Strategic Analysis*, 41(5), pp. 464 - 477. doi:10.1080/09700161.2017.1343235.
4. Bărgăoanu, A., Godzimirski, J., Ioniță, D. (2020). *Information warfare and information operations in The Black Sea area*. (N. S. Center, Ed.), newstrategycenter.ro: <https://www.newstrategycenter.ro/wp-content/uploads/2019/11/FLANKS-Working-Paper-Information-Warfare-And-Information-Operations-in-the-Black-Sea-Area.pdf>, retrieved on 12 August 2025.
5. Beznosiuk, M. (25 August 2025). *Atlantic Council*, Putin's hybrid war against Europe continues to escalate: <https://www.atlanticcouncil.org/blogs/ukrainealert/putins-hybrid-war-against-europe-continues-to-escalate>, retrieved on 25 August 2025.
6. Burlacu, P., Sandu, M.V. (2023). *Ukrainian USV (Uncrewed Surface Vessel) attack on ships of the Black Sea Fleet Lessons learned*. (M. P. Constanta, Ed.) *Scientific Bulletin of Naval Academy*, XXVI 2023(2), pp. 31-40. doi:10.21279/1454-864X-23-12-003.
7. Creswell, J., Creswell, D. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (5th ed., Vol. 1). California: SAGE Publications, Inc., https://spada.uns.ac.id/pluginfile.php/510378/mod_resource/content/1/creswell.pdf, retrieved on 20 August 2025.

8. Cucinschi, A.L. (2024). *The Suitability of Multi-Domain Operations for the Black Sea* (A.L. Reczkowski, Ed.). *GLOBSTATE Responding to contemporary challenges in security and operating environments strategy, operations, methodology*, 6(1), pp. 75-85, doi:https://cdissz.wp.mil.pl/u/documents/Responding_to_Contemporary_Challenges_in_Security_and_Operating_Environments_-_online_print_off_PGVURm1.pdf, retrieved on 22 August 2025.
9. Dalsjö, R., Jonsson, M., Norberg, J. (30 May 2022). *A Brutal Examination: Russian Military Capability in Light of the Ukraine War. Survival: Global Politics and Strategy*, 64(3), pp. 7-28. doi:10.1080/00396338.2022.2078044.
10. Deppe, C. (2023). *Disinformation in Cognitive Warfare Foreign Information Manipulation and Interference, and Hybrid Threats*. doi:10.5281/zenodo.10005172
11. Deppe, C., Schaal, G. (2024). *Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory concept*. doi:10.3389/fdata.2024.1452129.
12. Eckel, M. (20 August 2025). *Report: Russian Sabotage Operations in Europe Have Quadrupled Since 2023*, Radio Free Europe/Radio Liberty: <https://www.rferl.org/a/russia-sabotage-europe-hybrid-attacks/33508179.html>, retrieved on 24 August 2025.
13. Egeli, S. (25 June 2021). *Space-to-Space Warfare and Proximity Operations: The Impact on Nuclear Command, Control, and Communications and Strategic Stability*. doi:10.1080/25751654.2021.1942681.
14. Fenton, A.J. (19 March 2024). *Preventing Catastrophic Cyber-Physical Attacks on the Global Maritime Transportation System: A Case Study of Hybrid Maritime Security in the Straits of Malacca and Singapore*. doi:10.3390/jmse12030510.
15. Ferris, J. (2012). *Small wars and great games: The British Empire and hybrid warfare, 1700-1970*. In J. Ferris, *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present* (Vol. 1, pp. 199-224). Cambridge University Press. doi:10.1017/CBO9781139199254.008.
16. Florido-Benítez, L. (2024, 08 28). *The types of hackers and cyberattacks in the aviation industry*. In *Journal of Transportation Security*, 17. doi:10.1007/s12198-024-00281-9.
17. Gaber, Y. (2024). *A New Security Reality Strategic Approaches for the Wider Black Sea Region*, George C. Marshall European Center For Security Studies: https://www.marshallcenter.org/sites/default/files/files/2024-11/gaber_a-new-security-reality-clock-tower-final_20241105_1.pdf, retrieved on 21 August 2025.
18. Godzimirski, J., Mitrescu, S. (29 May 2025). *HYBRID FRONTLINES: Russian Threats and the Future of Maritime Infrastructure in the Black Sea and the North Sea*. (G. Scutaru, Ed.), caleaeuropeana.ro: https://www.caleaeuropeana.ro/wp-content/uploads/2025/05/WP1_versiune-finala-macheta.pdf, retrieved on 23 August 2025.
19. Gombar, M. (3 March 2025). *Algorithmic Manipulation and Information Science: Media Theories and Cognitive Warfare in Strategic Communication*, ej-media.org: <https://www.ej-media.org/index.php/media/article/view/41/59>, retrieved on 12 August 2025.
20. Grier, P. (2017). *The perils of hybrid wars*. In *Air Force Magazine*, 100(3), pp. 24- 29, <https://0k11m85ld-y-https-www-scopus-com.z.e-nformation.ro/pages/publications/85019186186>, retrieved on 23 August 2025.
21. Grossfeld, E. (2024). *Russia's Declining Satellite Reconnaissance Capabilities and Its Implications for Security and International Stability*. (Routledge) doi:10.1080/08850607.2024.2330848.
22. Headquarters, Department of the Army (2025). *FM 3-0 Operations*. Department of the Army. Department of the Army, https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN43326-FM_3-0-000-WEB-1.pdf, retrieved on 22 August 2025.

23. Hoehn, J. (2021). *Joint All-Domain Command and Control (JADC2)*. Congressional Research Service. Congress.gov., https://www.congress.gov/crs_external_products/IF/PDF/IF11493/IF11493.14.pdf, retrieved on 23 August 2025.
24. Höyhty, M., Uusipaavalniemi, S. (2023). *The space domain and the Russo-Ukrainian war: Actors, tools, and impact*. (H. CoE, Ed.), Hybrid CoE: <https://www.hybridcoe.fi/wp-content/uploads/2023/01/20230109-Hybrid-CoE-Working-Paper-21-Space-and-the-Ukraine-war-WEB.pdf>, retrieved on 14 August 2025.
25. Islam, M. (2024). *Maritime Diplomacy and Regional Cooperation Mechanisms: Insights from the Black Sea and Bay of Bengal*. *Millennial Asia*. doi:10.1177/09763996241256162.
26. Kohler, M. (2020). *The Joint Force Maritime Component Command and the Marine Corps Integrate to Win the Black Sea Fight*. In *Journal of Advanced Military Studies*, 11(2), pp. 88-105. doi:10.21140/mcu.20201102005.
27. Kunertova, D. (2023). *Drones have boots: Learning from Russia's war in Ukraine*. *CONTEMPORARY SECURITY POLICY*, 44(4), pp. 576-591. doi:doi.org/10.1080/13523260.2023.2262792
28. Łubiński, P. (2022). *Hybrid Warfare or Hybrid Threat – The Weaponization of Migration as an Example of the Use of Lawfare – Case Study of Poland*. *Polish Political Science Yearbook*, 51, pp. 43-55. doi:10.15804/ppsy202208.
29. Mitrescu, S., Sokolov, M. (2025). *In the Crosshairs: Hybrid Threats and the Challenge to Maritime Infrastructure*. In *NATO Science for Peace and Security Series C: Environmental Security* (Vol. Part F140, pp. 65-90). Springer Science and Business Media B.V. doi:10.1007/978-94-024-2300-6_6.
30. Monaghan, A., Connolly, R. (2023). *The sea in Russian strategy* (Vol. 1). Manchester: Manchester University Press.
31. North Atlantic Treaty Organization (February 2019). *Allied Joint Doctrine for the Conduct of Operations (AJP-3)*. (1), C, 164. NATO Standardization Office, https://www.coemed.org/files/stanags/01_AJP/AJP-3_EDC_V1_E_2490.pdf, retrieved on 22 August 2025.
32. North Atlantic Treaty Organization (June 2025). AJP-3.19, Allied Joint Doctrine for civil-military cooperation. *NATO Standardization Office (NSO)*(1), B, 62. NATO Standardization Office (NSO), https://www.coemed.org/files/stanags/01_AJP/AJP-3.19_EDA_V1_E_2509.pdf, retrieved on 22 August 2025.
33. Orde, K. (2016). *Lawfare: Law as a Weapon of War*. Oxford University Press. doi:10.1093/acprof:oso/9780190263577.001.0001.
34. Peled, R., Aizikovich, E., Habler, E., Elovici, Y., & Shabtai, A. (2023). *Evaluating the Security of Satellite Systems*, arxiv.org: <https://arxiv.org/pdf/2312.01330>, retrieved on 12 August 2025.
35. Plichta, M. (2025). *Precise Mass in Action. Assessing Ukraine's One-Way Attack Drone Campaign*. *RUSI*, 170(4), pp. 42-48. doi:10.1080/03071847.2025.2527923.
36. Proto, L., Lamoso-González, P., García, L.B. (2025). *The EU's FIMI Turn: How the European Union External Action Service Reframed the Disinformation Fight*. doi:10.17645/mac.9474.
37. Sabanadze, N., Dalay, G. (2025). *Understanding Russia's Black Sea strategy. How to strengthen Europe and NATO's approach to the region*, Chatham House: <https://www.chathamhouse.org/2025/07/understanding-russias-black-sea-strategy/03-threat-perceptions-and-failure-signalling>, retrieved on 22 August 2025.
38. Schaub, G., Murphy, M., Hoffman, F. (2017). *Hybrid maritime warfare building Baltic resilience*. In *RUSI Journal*, 162(1), pp. 32-40. doi:10.1080/03071847.2017.1301631.

39. Schmidt, D., Radke, K., Camtepe, S., Foo, E., & Ren, M. (2016). *A Survey and Analysis of the GNSS Spoofing Threat and Countermeasures*. *ACM Computing Surveys (CSUR)*, 48(4), pp. 1-31. doi:<https://doi.org/10.1145/2897166>.
40. Schwarz, M., Marx, M., Federrath, H. (2021). *A Structured Analysis of Information Security Incidents in the Maritime Sector*. doi:10.48550/arXiv.2112.06545.
41. Scutaru, G., Pavel, A. (2025). *Black Sea Region Security Assessment*. In *NATO Science for Peace and Security Series C: Environmental Security* (Vol. Part F140, pp. 29-38). Springer Science and Business Media B.V. doi:10.1007/978-94-024-2300-6_3.
42. Soldi, G., Gaglione, D., Rapone, S., Forti, N., d'Afflisio, E., Kowalski, P., ... Warner, C. (2023). *Monitoring of Underwater Critical Infrastructures: the Nord Stream and Other Recent Case Studies*. doi:10.48550/arXiv.2302.01817.
43. Stensrud, C.J., Østhagen, A. (2024). *Hybrid Warfare at Sea? Russia, Svalbard and the Arctic*. In *Scandinavian Journal of Military Studies*, 7(1), pp. 111-130. doi:10.31374/sjms.233.
44. Tagarev, T. (2021). *Understanding Hybrid Influence: Emerging Analysis Frameworks*. *Studies in Big Data*, 84, pp. 449-463. doi:10.1007/978-3-030-65722-2_29.
45. Todorov, Y. (2024). *Navigating Uncharted Waters: Tackling Maritime Cybersecurity Challenges in the Black Sea Region*. *Information & Security*, 55(2), 113-132. doi:10.11610/isij.5509.
46. US Air Force (2021). Air Force Doctrine Publication 1: The Air Force. *Air Force Doctrine Publication 1: The Air Force*, 1, 1, 20. Center for Doctrine Development and Education, https://www.doctrine.af.mil/Portals/61/documents/AFDP_1/AFDP-1.pdf, retrieved on 22 August 2025.
47. US Army Training and Doctrine Command (2018). The U.S. Army in Multi-Domain Operations 2028 (TRADOC Pamphlet 525-3-1). 100. TRADOC, <https://adminpubs.tradoc.army.mil/pamphlets/TP525-3-1.pdf>, retrieved on 12 August 2025.
48. US Navy (2025). SURFACE WARFARE: THE COMPETITIVE EDGE 2.0. *SURFACE WARFARE: THE COMPETITIVE EDGE 2.0*, 1, 2, 32. Commander, Naval Surface Force, US Pacific Fleet, <https://www.surfpac.navy.mil/Portals/54/Documents/CNSP/SNA/SNA-2025/THE%20COMPETITIVE%20EDGE%202.0%20Jan%203%20Print%20Final.pdf>, retrieved on 20 August 2025.
49. US Space Force (2025). Space Force Doctrine Document – 1 (SFDD-1), The Space Force. (1), 1, 51. Space Training and Readiness Command (STARCOM), https://www.starcom.spaceforce.mil/Portals/2/Space%20Force%20Doctrine%20Document%201%20FINAL_4Apr25.pdf, retrieved on 20 August 2025.
50. Usewicz, T., Keplin, J. (2023). *Hybrid Actions and Their Effect on EU Maritime Security*. In *Journal on Baltic Security*, 9(1), pp. 32-68. doi:10.57767/jobs_2023_001.
51. Vdovychenko, V., Albu, N., Chitadze, N. (2024). *Navigating the Trilemma of (In) security: Strategic Competition in the Black Sea Region*. *Center for Defence Strategies, Ukraine*, 23(2), pp. 117-128. doi:10.11610/Connections.23.2.08.
52. Wither, J. (2023). *Hybrid Warfare Revisited: A Battle of 'Buzzwords'*. *Connections*, 22(1), pp. 7-27. doi:10.11610/Connections.22.1.02.
53. Zorri, D., Kessler, G. (2024). *Position, Navigation, and Timing Weaponization in the Maritime Domain: Orientation in the Era of Great Systems Conflict*, National Defense University Press, <https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3678180/position-navigation-and-timing-weaponization-in-the-maritime-domain-orientation>, retrieved on 22 August 2025.

USING CYBER RANGES IN CYBERSECURITY TRAINING AS AN ACTION PLAN IN THE FACE OF HYBRID THREATS

Major General Stayko PROKOPIEV

Commandant of the Rakovski National Defence College, Sofia, Bulgaria

Associate Professor Dr. Veselina ALEKSANDROVA

Rakovski National Defence College, Sofia, Bulgaria

Dr. Elitsa PAVLOVA

University of National and World Economy, Sofia, Bulgaria

Dr. Violeta VASILEVA

Future Innovation Labs, Sofia, Bulgaria

DOI: 10.55535/RMT.2025.3.19

Cyber ranges are key tools for developing effective strategies and tactics to protect against hybrid threats, which combine traditional military methods with cyberattacks. In this scientific paper, the authors examine the significance of using cyber ranges in cybersecurity training, analysing their architecture, main principles of design and implementation, and their lifecycle. The question of how these platforms can be used to enhance strategic resilience and national defence through simulating various scenarios and vulnerabilities is explored. Specific recommendations for integrating cyber ranges into action plans against hybrid threats are also provided. The employment of cyber ranges for the preparation of personnel, organizations, and consequently states can increase their readiness and capability to respond to complex and multifaceted hybrid threats, ensuring better protection of their critical infrastructures and information systems. This approach not only supports strategic resilience and strengthens national defence but also creates a foundation for international cooperation and knowledge exchange in the field of cybersecurity.

Keywords: hybrid threats; cyber range; cybersecurity; strategic resilience;

INTRODUCTION

In recent years, we have witnessed a rapid development of information technologies and cyberspace, which, as a global phenomenon, has changed the characteristics of the behaviour of individual societies and individual citizens in particular. The Internet, as a global network affecting all spheres of public life, is becoming not only the largest repository of information, but also the place where a significant potential of critical infrastructure and services at the state and corporate levels is concentrated. The global network is becoming an increasingly significant factor for national security and defence. All this leads to new challenges and hybrid threats in cyberspace, which are characterized by high dynamics, complexity and unpredictability. The development of offensive capabilities for conducting large-scale cyber operations by terrorist and extremist organizations, as well as by individual state entities, as a tool for achieving destructive and inhumane objectives against society and citizens, is one of the main reasons for rethinking the role of cyberspace as an element of hybrid threats and a fifth domain of conflicts and interaction.

The increase in risks and threats in the geopolitical and strategic security environment, as well as in cyberspace, creates conditions for increasing the vulnerabilities of military communications and information systems for command and control. There is a need for effective and timely implementation of protection measures for own systems as well as for the development of cyber defence capabilities compatible with those of NATO member states. Cyber security requires resources, such as material, human, financial and technological ones.

At the NATO Summit in Warsaw in 2016, cybersecurity was identified as one of the main priorities of the organization. Priority areas were also identified, such as building the Alliance's collective capabilities, including cyber defence in the planning process, and increasing member states' investments in this area. It is because, for many years, armed struggle and war have been waged in four physical domains that objectively exist – on land, in the air, in the maritime space, and in space. After the Warsaw meeting, the fifth domain – cyberspace – is defined (Grigorov, 2016).

In the transition to network-centric capabilities, high-tech systems for command and control of troops, intelligence, targeting and control of intelligent weapons, the dependence of our systems is actually becoming very high. For example, if cyber operations lead to the inoperability of the global positioning system (GPS), all missile

systems that are guided and controlled by GPS will not be able to function. Cyber operations can lead to catastrophic consequences if, during a military operation, the armed forces have not taken appropriate measures to protect their own command, control, guidance and attack systems. That is why NATO has identified cyberspace as the fifth domain, important for defence.

It is necessary to develop policies and guidance documents for the Armed Forces cyber defence in accordance with the consideration of cyberspace as the fifth domain. It is related to strategic sustainability, national defence and the need to actively counter hybrid threats, cyber attacks and hybrid wars.

For this purpose, the opportunities of our membership in NATO and the EU can be used to participate in joint initiatives to build common capacity and capabilities; to share information on cyber incidents and mutual assistance with state institutions and international organizations in a coordinated manner; to cooperate with the business and academic community; to achieve expert capacity in cybersecurity and to increase preparation through periodic training and participation in cyber exercises with cyber polygons.

CYBER RANGE ARCHITECTURE

The cyber range architecture includes a work platform, a user interface, scenarios, projects and infrastructure, and teams. The user interface forms a realistic cyberspace consisting of real devices and virtual machines. Registration in the platform covers the functions of the instructor and participant profile elements, respectively.

The platform consists of a set of technologies used as a foundation on which applications, processes, and services can be developed. The platform contains the main elements that provide automated processes such as creating virtual machines, simulating network traffic, installing software packages, mass creating network user accounts, monitoring the state of the workspace, and visualizing information for instructors and participants. The elements can be developed or implemented using, customizing, and configuring open-source solutions. However, they must comply with standards to ensure their interoperability and reuse.

The main elements of the cyber range platform are related to:

1. *Tracking.* The platform must be able to track the status of the workspace elements, extracting information related to the status of services, processes, applications and software updates; creating and deleting users (including user rights and sessions) and files; firewalls; intrusion detection systems; network traffic data.

2. *Registry*. The registry manages the platform database, which maintains participant records according to data obtained from tracking and those submitted by the “Instructor”.
3. *Feedback and reports*. Feedback and reports visualize data on the evolution of cyber attacks occurring in a given exercise; changes in the results of the teams participating in a given course; team score; workspace elements. Visualization of training data is key to improving the effectiveness of exercises.
4. *Automation*. The element includes mechanisms that automate the workspace functions for generating network traffic, virtual user accounts that perform virtual actions, and automated cyberattacks. Generating network traffic enhances the realism of the platform. Network traffic generators should simulate traffic of various protocols (e.g. HTTP – HyperText Transfer Protocol, SMTP – Simple Mail Transfer Protocol, POP – Post Office Protocol, FTP – File Transfer Protocol, ICMP – Internet Control Message Protocol) and provide means for specifying the source, destination, duration, and amount of generated traffic.
5. *User interface*. The space is created in an automated manner based on the scenario selected by the instructor and downloaded from the scenario repository. The workspace elements are interconnected with the platform elements and include virtual or physical computers, mobile devices, network devices, servers, services, integrated technologies, wireless networks etc.

User Interfaces

The user interfaces for instructors and participants provide various capabilities, which are shown in *table 1*.

Table 1: Cyber range instructor and participant user interface capabilities (authors’ design)

Functionality / UI element	Instructors	Participants
Dashboard	View sessions, participant status, exercise results	Personal progress, upcoming tasks, current level
Scenarios and missions	Create, configure and manage scenarios	Access scenarios, execute missions, report results

Functionality / UI element	Instructors	Participants
Real-time monitoring	Tracking of participants' actions and network traffic in the simulated environment	Visualization of their own actions and their consequences on the system
Analysis and reports	Generation of individual and group reports, assessment of skills	Access to personal report and recommendations for improvement
Communication module	Built-in chat, ability to send instructions and feedback	Built-in chat for questions, team collaboration
Gamification	Setting criteria for points and achievements	Accumulation of points, achievements, comparison with other participants
Integration with external systems	Adding real cyber threats and actual attacks for training	Accumulation of points, achievements, comparison with other participants
Role and access management	Defining access levels and roles	Access only to training missions and own results
Interactive labs	Setting up virtual environments for different scenarios	Practical exercises in a secure simulation environment
Feedback and assessment	Direct feedback, individual comments	Possibility of self-assessment and receiving personalized recommendations

Scenarios

Scenarios are created by combining tasks, conditions, goals, and learning materials that are stored in a repository. Scenario elements include: virtual machines and network devices used as templates during workspace creation; scripts for creating and deploying the workspace; configuration files for platform elements. A scenario defines the steps that participants must follow to complete the exercise. Each step includes sub-goals, a set of conditions, and learning elements. Attributes are set that describe the details of the scenario, including name, description, difficulty level, and complexity.

Teams

Teamwork helps to evaluate attack scenarios in real-world conditions (Yamin, 2020). The red and blue teams are common to all cyber polygons. The red team carries out the attack on users' computers using viruses, malware, and more, designed by the white team. The green team is responsible for simulating wired or wireless connections between users and their computers or smartphones to the network infrastructure. The blue team members take on either the role of defenders of the system, protecting it from cyberattacks, or the role of investigators of a cyberattack and its consequences. The white team creates cyberattack scenarios in order to track the success or failure of the blue team. The yellow team reports situational awareness by reproducing innocent users compromising the security of the network. Some cyber polygons use a grey and purple team. The grey represents normal traffic and service requests to be supported, and the purple is a collaboration between the red and blue teams responsible for protective techniques.

During the exercise, the instructor gives advice related to the learning content and receives information from the tracking elements, checks whether the learners have managed to perform the appropriate actions within the allotted time, and evaluates them.

BASIC PRINCIPLES FOR SELECTING AND IMPLEMENTING CYBER RANGE

The design and implementation of cyber ranges should be guided by several core principles to ensure maximum educational value and replicate the operational dimensions of cybersecurity challenges (Hart et al., 2020).

❖ Accuracy and Realism

Training environments are essential for developing skills that are directly transferable to operational contexts. Cyber ranges should accurately replicate network topologies, system configurations, services and applications with realistic performance characteristics and constraints, typical user activities and business processes within which to detect security-related events. Similarly, adversary behaviour should reflect documented tactics, techniques and procedures of real-threat actors. Realistic representation of the impacts of both successful attacks and defensive measures helps trainees understand events relevant to their decisions – business impacts, service disruptions that may arise from security incidents or mitigation actions. Technical accuracy ensures that skills acquired during training can be directly applied to real-world scenarios.

❖ **Scalability and Flexibility**

The dynamic nature of cybersecurity requires learning environments that can adapt to a variety of needs. Cyber range must work with varying numbers of participants, from individual training to large-scale team exercises involving dozens or hundreds of participants. Learning platforms must support scenarios of varying complexity, from focused skill-building exercises to comprehensive incident response simulations. The environment must be configurable to represent different business sectors, organizational structures, and technical architectures.

❖ **Insulation and Security**

Proper containment is essential for both security and educational purposes. Complete *network separation* ensures that malicious activities in the learning environment cannot affect production systems. *Data isolation* means that learning environments should use synthetic or properly sanitized datasets. Learning environments should replicate the characteristics of production data without exposing sensitive information. *Robust authentication and authorization mechanisms* are needed to restrict access to appropriate learning scenarios and system components based on learner roles and permissions. Another important part is *logging and monitoring systems* that track all activities in the learning environment. Mechanisms to *prevent unauthorized extraction* of tools, techniques, or scenarios from the learning environment help protect intellectual property and prevent potential misuse of learning materials.

❖ **Reproducibility and Standardization**

Consistent learning experiences require systematic approaches.

RECOMMENDATIONS FOR INTEGRATING CYBER RANGE INTO HYBRID THREAT RESPONSE PLANS

Hybrid threats pose complex and multifaceted challenges that require coordinated and adaptive response strategies. In the context of modern strategic resilience and national defence, cyberspace plays an increasingly important role as an arena for conflicts and attacks. One of the effective methods for preparing for and responding to these threats is the use of cyber ranges – virtual environments that simulate real-world conditions and scenarios. Specific recommendations for integrating cyber ranges into hybrid threat response plans include the following:

Development of Realistic Scenarios. The first step towards successfully integrating cyber ranges is the development of realistic scenarios that reflect potential hybrid threats. These scenarios should include combinations of physical, informational

and psychological attacks, as well as interactions between different actors (government, private sector, civil society). It is important that the scenarios should be updated regularly to reflect new trends and tactics of adversaries.

Training and Simulations. Cyber ranges provide a unique opportunity to conduct training and simulations that prepare personnel for real-world situations. These exercises may include incident detection and response training, crisis management, and inter-agency coordination. Training should be systematic and periodic to ensure ongoing readiness and skill development.

Cooperation and Coordination. Effective countermeasures against hybrid threats require close cooperation between various stakeholders. Cyber ranges can serve as platforms for joint exercises and information exchange between government institutions, private companies, and international partners. This cooperation not only improves interoperability, but also builds trust and mutual understanding between participants.

Technological Readiness and Infrastructure. The successful integration of cyber ranges requires the availability of an appropriate technological infrastructure. It includes high-performance computer systems, simulation software, and data analysis tools. In addition, reliable communication channels and secure networks must be provided to ensure information security and continuity of operations.

Monitoring and Evaluation. The integration of cyber ranges into hybrid threat response plans should be subject to ongoing monitoring and evaluation. It includes analysing the results of simulations, identifying weaknesses and gaps, and implementing corrective measures. Regular review and updating of procedures and policies ensure their effectiveness and adaptability to changing conditions.

THE MAIN CHALLENGES IN DESIGNING AND IMPLEMENTING A CYBER RANGE

The main challenges in designing and implementing a cyber range are related to the high costs of preparation, high requirements for testing, building a learning strategy and evaluation. The preparation phase requires many resources, specialized personnel, as well as a long period of time. According to a study on the evaluation of cyber defence exercises using a visual analysis process, a cyber range should be a safe, legal and isolated environment from external networks and the Internet (Ošlejšek, 2018). For this reason, special attention needs to be paid to the installation of applications and tools, the construction of network services, the provision of controlled access to the Internet, as well as the involvement of specialized

personnel to test and make optimizations and adjustments. Another challenge facing educational cyber ranges is that they must be based on good teaching practices including learning objectives, participant characteristics etc. Cybersecurity training requires the formation of an interactive and multi-layered learning environment. Exercise scenarios must meet the needs and experience level of the learners. The integration of emerging technologies such as artificial intelligence and digital twins is transforming traditional approaches, while standardization efforts continue to develop worldwide.

CONCLUSIONS

In conclusion, it can be summarized that integrating cyber ranges into hybrid threat response plans is a key element for enhancing national and international security. By developing realistic scenarios, conducting training and simulations, promoting cooperation, providing the necessary technological infrastructure, and continuous monitoring and evaluation, the ability to prevent and respond to complex threats can be significantly improved. Effective cyber ranges require modular, scalable architectures with high-quality simulations and adherence to established pedagogical frameworks and comprehensive evaluation mechanisms.

Cyber ranges represent a powerful tool that can help organizations and states address the challenges in the face of hybrid threats to achieve strategic resilience and national defence.

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. Grigorov, M. I. (2 December 2016). *Petiyat domeyn i zaplahite v kiberprostranstvoto*, <https://armymedia.bg/2016/12/02/петият-домейн-и-заплахите-в-киберпрос/>, retrieved on 10 September 2025.
2. Ošlejšek, R. J. (2018). *Evaluation of Cyber Defense Exercises Using Visual Analytics Process*. EEE Frontiers in Education Conference (pp. 1-9). doi:<https://doi.org/10.1109/FIE.2018.8659299>.

3. Hart, S., Margheri, A., Paci, F., Sassone, V. (2020). *Riskio: A Serious Game for Cyber Security Awareness and Education*. Computers & Security, 95, 101827. doi:<https://doi.org/10.1016/j.cose.2020>.
4. Yamin, M. M. (2020). *Cyber ranges and security testbeds: Scenarios, functions, tools and architecture*, 101636. Computers & Security (88).

METHODS USED BY THE RUSSIAN FEDERATION TO CIRCUMVENT INTERNATIONAL SANCTIONS IMPOSED BY THE INTERNATIONAL COMMUNITY

Police Quaestor Associate Professor Dr. Cătălin ANDRUȘ

Director of the National College of Home Affairs, Bucharest

Colonel (r.) Dr. Lucian IVAN

Assistant Professor at the National College of Home Affairs, Bucharest

DOI: 10.55535/RMT.2025.3.20

Following the Russian Federation's unjustified attack on Ukraine in February 2022, the international community reacted firmly and successively imposed international sanctions against the Kremlin regime. In order to force the Russian Federation to comply with international law and stop this unjustified military conflict, these sanctions must be rigorously implemented at the level of democratic states so as not to provide the authoritarian regime in Moscow with the resources necessary to continue the military conflict in Ukraine indefinitely. The Russian Federation has reacted to these international sanctions by deciding to cooperate with other sanctioned states, to negotiate new contracts for the distribution of its energy resources, to use proxies to obtain military and dual-use products and technologies necessary for its own defence industry etc. To counteract these measures, democratic states must strengthen the international sanctions regime imposed on the Russian Federation by eliminating systemic vulnerabilities, including measures to sanction states that support Russia, and identifying the best methods to prevent the authoritarian regime in Moscow from circumventing international sanctions.

Keywords: international sanctions; dual use; circumvention measures; energy resources; sanctions regime;

INTRODUCTION

Immediately after the Russian Federation's unjustified attack on Ukraine in February 2022, the Western democratic community took firm action to impose sanctions against the autocratic authorities in Moscow, with the aim of supporting Ukraine in its defence against Russia's unprovoked aggression. Against the backdrop of the ever-increasing costs of the war, the economic sanctions imposed on the Russian Federation as part of the Western states' response to this unprovoked and illegitimate invasion are increasingly destabilising the Russian economy, these challenges being important for the authorities in Moscow in the peace negotiations process.

Although international sanctions have had an effect on the Russian Federation's economy, Russian exporters, particularly those in the energy sector (oil and natural gas), have managed to find buyers for these resources outside Western countries. Thus, these energy importers play a significant role in supplying the Russian Federation with foreign currency, which allows the Russian authorities to continue financing the military conflict in Ukraine.

It can be said that the West, especially the European Union, which was the Russian Federation's main partner until 2022, has not shown sufficient determination and political will to rigorously enforce international sanctions. In this context, Russia continues to have the goods and technologies it needs to continue the military conflict in Ukraine. Although it is impossible to completely stop all the channels used by the Russian Federation to circumvent international sanctions, it is possible to identify viable solutions to limit these activities by the Moscow authorities by increasing costs for Russia and extending delivery times.

In this context, Western action should focus on three areas of interest, namely: strengthening financial sanctions, including by imposing sanctions on entities in third countries that violate international regulations; prioritising the implementation of restrictions within the EU, in particular by eliminating operational loopholes and reducing or eliminating supply channels for products and technologies that can be used in the Russian defence industry, and further reducing the Russian Federation's revenues, in particular those generated by the energy sector, by combating the circumvention of sanctions by Russian companies and completely eliminating Western countries' dependence on Russian energy resources.

While some countries, such as China, the Islamic Republic of Iran and North Korea, openly support the Russian Federation in violating international sanctions mainly for ideological reasons, other countries, such as Turkey, do so for profit. The European Union must therefore focus its diplomatic efforts on these countries, including by extending the use of secondary sanctions to them.

SANCTIONS IMPOSED BY WESTERN STATES ON THE RUSSIAN FEDERATION

After the Russian Federation's unprovoked invasion of Ukraine in February 2022, the international community reacted immediately, with 141 UN member states strongly condemning Russia's invasion of Ukraine by voting, on 2 March 2022, for a General Assembly resolution condemning the actions of the Moscow authorities (UN, 2022). Of these 141 states, only 39 imposed economic restrictions on the financial and technological capacity of the Russian Federation with the aim of making it impossible to continue the war in Ukraine (EU member states and G7 member states, in particular the USA, the United Kingdom of Great Britain and Northern Ireland, Canada and Japan) (European Commission, 2022, p. 1). The extent of the sanctions imposed on Russia by each state varied substantially depending on political and economic interests. The strictest restrictions against the Russian Federation were adopted by the USA, which, in addition to financial, trade and individual sanctions directly targeting Russian entities, also imposed secondary sanctions against entities in third countries that do not comply with the sanctions imposed by the USA. This radical and effective approach adopted by the USA must also be adopted by the EU and other Western states in order to persuade the authorities in Moscow to end the war in Ukraine as soon as possible (Wisniewska, 2023-1).

The main objective of international sanctions targeting Russian imports was to reduce the Russian Federation's revenues and budget revenues in order to limit its ability to finance the war in Ukraine. An important aspect was the EU Member States' renunciation of Russian energy resources. Whereas, prior to the outbreak of the military conflict in Ukraine, the EU was heavily dependent on Russian natural gas and the countries of Central and Eastern Europe were largely dependent on Russian energy resources, there has now been a substantial reduction in dependence on these resources. Of course, giving up Russian energy resources has also had negative effects in certain EU Member States, mainly Germany, which have been forced to import natural gas and oil at significantly higher prices. As a result, the economic competitiveness of companies in these countries has declined due to rising production costs, leading to lower sales and, implicitly, to economic crisis.

The international sanctions mainly targeted the following areas:

- **Arms** – The sanctions imposed by Western countries prior to the February 2022 attack on Ukraine in this area were supplemented by the inclusion of equipment, components and machine tools necessary for arms production. The first joint list of products and technologies subject to international sanctions was drawn up on 3 March 2022 and, in the following period the list was expanded, with several states committing to comply with the sanctions regime imposed on the Russian Federation. Thus, by December 2024, the coalition that imposed restrictive measures against the Moscow regime comprised 39 states, and the list contained 50 categories of products and technologies (e.g. integrated circuits and the machinery used to manufacture them, drones, optical equipment, communications technologies, bearings) (European Commission, 2024). In addition to these restrictive measures, restrictions have been imposed since July 2014 on certain military and dual-use products and technologies. Furthermore, following the annexation of Crimea in March 2014, the USA prohibited American companies from cooperating with many Russian companies operating in the defence sector.
- **Energy** – sanctions include a ban on the supply of technologies necessary for the liquefaction of natural gas, as well as the provision of specialised services related to the development of oil and natural gas extraction.
- **Aviation and space** – sanctions relate to the supply of fuel for aircraft, aeroplanes and helicopters, as well as spare parts for them. Maintenance or repair services for aircraft and helicopters are also subject to sanctions.
- **Transport** – the restrictions concern the supply of rolling stock, including locomotives, as well as other means of transport (e.g. trucks). Repair and maintenance services for these products are also subject to sanctions.
- **IT sector** – international sanctions target the supply of electronic and optical components, cameras and production management software, as well as the provision of related services.

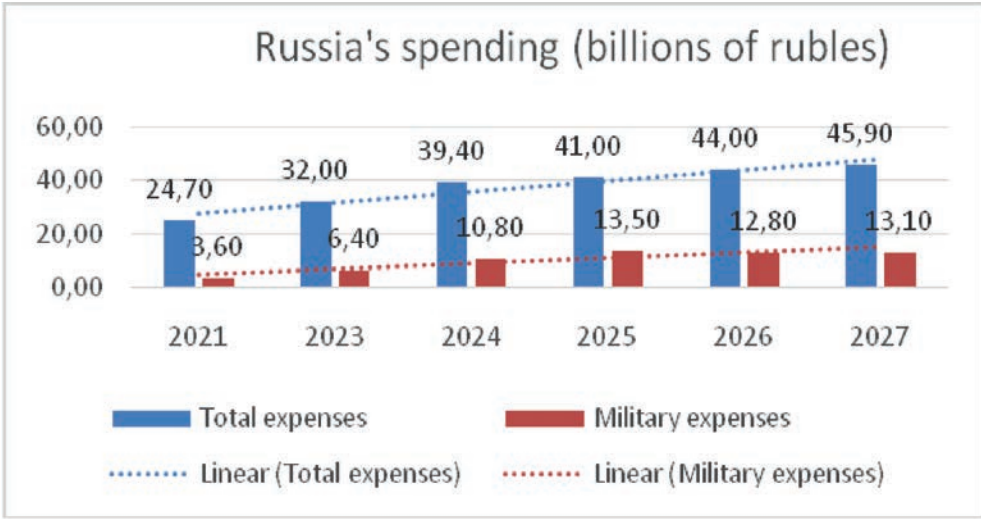
The restrictive measures also targeted the export of luxury goods (e.g. watches, jewellery, alcoholic beverages), and the list of sanctions included certain companies and large-scale investment projects (e.g. Arctic LNG), mainly targeting the arms and energy sectors, as well as Russian companies operating in these areas of strategic interest to the Moscow authorities. Another very important aspect is the freezing of Russian companies' assets in Western countries and the prohibition of Western companies from conducting financial transactions with them.

The sanctions imposed by Western countries against the Russian Federation must be rigorously enforced in order to limit the Moscow authorities' ability to obtain the funds necessary to continue the conflict in Ukraine. Although the restrictive measures were imposed in a timely manner by Western countries, the Moscow authorities have identified ways to circumvent them, which has led to the creation of parallel networks responsible for importing the products, equipment and technologies needed by the Russian Federation to continue the military conflict, including with the support of states friendly to Russia (e.g. China, the Islamic Republic of Iran, North Korea).

METHODS OF CIRCUMVENTING INTERNATIONAL SANCTIONS BY THE RUSSIAN FEDERATION

In order to circumvent international sanctions, the Russian Federation has used a variety of ingenious methods which, for a certain period of time, have allowed the import of products subject to sanctions. This process of avoiding international sanctions continues today, with the Russian Federation taking advantage of legislative vulnerabilities in certain countries or opportunities offered to companies in third countries to make substantial profits. From the point of view of the danger of the continuation of the military conflict in Ukraine, the most dangerous are military and dual-use products that are used in the Russian military-industrial complex. Although economically developed countries in the Euro-Atlantic area have mature systems for controlling exports of strategic products and technologies (military and dual-use), there have been cases where legal procedures have been circumvented by the use of shell companies in countries that are not subject to international sanctions. In this context, careful verification of intermediary companies is required, both by the responsible authorities in Euro-Atlantic states and by exporting companies, which should implement an internal control system capable of verifying importing companies.

The Russian Federation's military sector has grown rapidly since the invasion of Ukraine. The authorities in Moscow have planned to allocate approximately USD 135 billion to national defence, representing approximately 33% of total government expenditure. At the same time, preferential loans and extra-budgetary support from the Russian Federation's National Social Assistance Fund were granted to finance the defence industry.



Graph 1: Russian Federation expenditure on national defence¹

As can be seen in *graph 1*, the Russian Federation’s military expenditure will increase until 2027, which reveals the Moscow authorities’ interest in strengthening their defence industry in order to continue the military conflict in Ukraine or even extend the military conflict to other states. In this context, to counterbalance the Russian Federation’s armament, NATO agreed to increase military spending to 3%, and the EU took measures to supplement the military spending of member states by launching various programmes aimed at modernising the military-industrial sector (e.g. SAFE).

The Russian military sector does not comply with market economy principles, as the prices of military equipment are set arbitrarily and defence companies are paid in advance from the state budget. Due to the enormous demand from the Russian armed forces, it accepts everything that the Russian military complex can produce, regardless of the quality of the military equipment.

Official Russian statistics prior to the outbreak of the war in Ukraine revealed that the Russian Federation’s military sector depended on imports for approximately 10% of its needs, with the necessary products being technologically advanced, namely advanced electronics and optical systems. In 2015, after the introduction

¹ The source of the data is the State Duma of the Russian Federation and the Ministry of Public Finance of the Russian Federation. For 2022, national defence expenditure has not been made public. The data for 2023 were taken from the Russian Federation Budget Law adopted in December 2022, the data for 2024 were taken from the Budget Law adopted in November 2023, and the data for 2025, 2026 and 2027 were taken from the Draft Budget Law adopted in November 2024 (A.N.).

of the first international sanctions against the Russian Federation targeting the arms industry following the illegal occupation of the Crimean Peninsula, Russia's deputy minister of defence, Yuri Borisov, mentioned 826 military products whose manufacture required parts and technologies imported from Euro-Atlantic countries. It highlights the degree of dependence of the Russian military industry on imports from Euro-Atlantic countries, a percentage that has fallen significantly since February 2022. In the first half of 2023, the value of deliveries of goods essential for the production of military equipment fell by about 40%, while the value of deliveries of dual-use products fell by about 30%. The products most difficult for the Russian military complex to replace are aircraft and space navigation instruments, control devices, data transmission and reception stations, and integrated circuits, the value of which fell by more than 50% (Simola, 2023).

With regard to products and technologies used by the military that are subject to international sanctions, the Russian Federation has strengthened its cooperation with countries that have not adopted the sanctions regime, primarily China and, to a lesser extent, Hong Kong. Turkey, Malaysia, Kazakhstan, Kyrgyzstan and Armenia also played an important role (Pierzchala, 2024). Although Russia has not released data and information on its defence system, according to SIPRI estimates, in the period 2022-2023, the value of imported military equipment amounted to approximately USD 130 million, less than the maximum value recorded in 2014 (USD 200 million), but significantly more than in the years immediately following the military invasion of Ukraine, when those imports were minimal (SIPRI, 2025).

In the first phase, in order to circumvent international sanctions, the Russian Federation made legislative changes regarding import duties on certain products. Thus, in April 2022, Russia exempted goods brought into the country by individuals from customs duties up to the amount of EUR 1,000. In this context, citizens imported household appliances, electronics and perfumes on a large scale, not only for personal use, but also for resale on the domestic market. At the same time, depending on market demand, customs duties were substantially reduced, sometimes even to zero, including for electronic components, construction materials, pharmaceutical raw materials and paper, which not only covered the existing market deficit but also reduced the purchase prices of these scarce products (Eurasian Economic Commission, 2022).

On 30 March 2022, the Russian Federation legalised parallel imports, i.e. the import of products manufactured without the express consent of the trademark owner, this mechanism being imposed against the backdrop of foreign companies withdrawing from the Russian market. In the first two years of operation of this illegal

trade mechanism, products worth approximately USD 70 billion were imported. These parallel imports were carried out through countries that did not join the coalition of countries that imposed sanctions on the Russian Federation, in particular China (where large Western companies have production facilities), but also Hong Kong, Turkey (especially clothing) and Singapore (especially electronic products). In addition to these countries, the USA also mentioned the following countries that were most frequently used to circumvent international sanctions imposed on the Russian Federation and the Republic of Belarus: South Africa, Armenia, Brazil, the United Arab Emirates, Georgia, India, Kazakhstan, Kyrgyzstan, Mexico, Serbia, Taiwan, Tajikistan and Uzbekistan (Kommersant, 2024). In many cases, the goods did not physically reach these countries, as the products were diverted directly by Russian companies to the Russian Federation. In these situations, only the documents were drawn up by companies in the aforementioned countries, with the products being transported directly to Russia and the intermediary companies intentionally not declaring the final destination of the imported products. Thus, third countries were used primarily as transit points for goods subject to international sanctions, with the aim of concealing their final destination and substantially reducing logistics costs.

Under pressure from Western states, Turkey, which was an important logistics hub and a favourite route for Russian companies, banned the transit of products subject to international sanctions in March 2023 (Michalski, 2023). In Central Asia, imports that were initially made directly by the Russian Federation were brokered by companies in Kazakhstan or Kyrgyzstan, and products subject to international sanctions remained on Russian territory (Yle News, 2023). This route was also eliminated by the EU, which strengthened the sanctions regime for dual-use goods and technologies, prohibiting their transit through the Russian Federation. Another vulnerability that has been exploited by the Russian authorities is that the states through which dual-use products transit do not control shipments of such products and do not verify their final destination. To solve this problem, it is necessary for these countries to amend their legislation on the control of dual-use goods and technologies in order to control their transit and transshipment.

At the same time, the Russian Federation has used companies established in third countries (shell companies) for the re-export of products subject to sanctions. The interposition of these companies in the exporter-intermediary-final recipient chain has allowed the Russian Federation to illegally purchase products needed by the Russian military complex for the production of military equipment used in the conflict in Ukraine. In general, these companies are owned or controlled through intermediaries by Russian entities, their purpose being to import products

and technologies from the West and subsequently deliver them to the Russian Federation. Thus, it should be noted that, after the outbreak of the military conflict in Ukraine, the number of Russian-owned companies in Russia's neighbouring countries has increased significantly. This method involves significant additional costs, given that Russian-owned companies are required to pay taxes and duties in third countries. In this context, the Moscow authorities have held negotiations with third countries to obtain favourable financial conditions for Russian companies conducting commercial operations in these countries. This method is evidenced by the exponential growth in trade between the aforementioned countries, Western countries and the Russian Federation (Chupilkin, 2023).

In many cases, the Moscow authorities have created chains of intermediary entities with which they have managed to cover several countries, particularly for the import of dual-use products (Cook, 2023). Using this method, the Russian Federation has managed to purchase equipment from the USA and EU Member States, which was subsequently used to assemble weapons used in the military conflict in Ukraine (Tkachova, 2024). Statistics on exports of products subject to international sanctions to Southeast Asia, Turkey, the Persian Gulf states and Kazakhstan have increased significantly, indicating that some of these products have reached Russia through entities in the aforementioned states (Pierzchala, 2024).

The authorities in Moscow also took advantage of the lack of harmonisation between the sanction regimes imposed on the Russian Federation and Belarus. Thus, the massive export of cars from EU Member States to the Republic of Belarus, recorded until mid-2024, was largely destined for the Russian market, which was subject to sanctions on car imports (Kłysiński, 2024). Another illegal method used by Russian companies was to use incorrect customs codes in the classification of goods that were not on the control lists in order to circumvent export controls in accordance with the customs codes of the Harmonised System.

The sector most affected by international sanctions was the aviation industry, which was heavily dependent on equipment deliveries from major Western companies. The Russian aviation industry was unable to import specific equipment or produce it domestically. Under these circumstances, companies in the aviation industry proceeded to "*cannibalise*" certain aircraft by using their parts to repair other aircraft. The pressure on the Russian aviation industry was reflected in a sharp increase in aviation incidents in the country in 2023, with their number tripling during the reference period. Components were also imported from China, Tajikistan, Kyrgyzstan, Turkey and the United Arab Emirates. At the same time, the Russian Federation purchased aircraft, in particular small training aircraft (e.g. Cessna)

and passenger aircraft (e.g. Bombardier). In 2024, at least 28 aircraft were imported into Russia, mostly from Turkey (11), but also from Western countries, namely Germany and Sweden (Verstka Media, 2025).

One of the sectors that has not yet managed to recover is liquefied natural gas (LNG), with international sanctions in this area proving effective. Novatek has managed to complete a production line as part of the Arctic LNG 2 project with a delay of about one year. However, the company is unable to deliver LNG due to difficulties in accessing gas transporters, as sanctions targeting the Arctic LNG 2 project have discouraged foreign companies from cooperating in LNG transport. In this context, the construction of the other two production lines of the Arctic LNG 2 project is delayed, and the viability of the project is currently at risk (Rudnik, 2024).

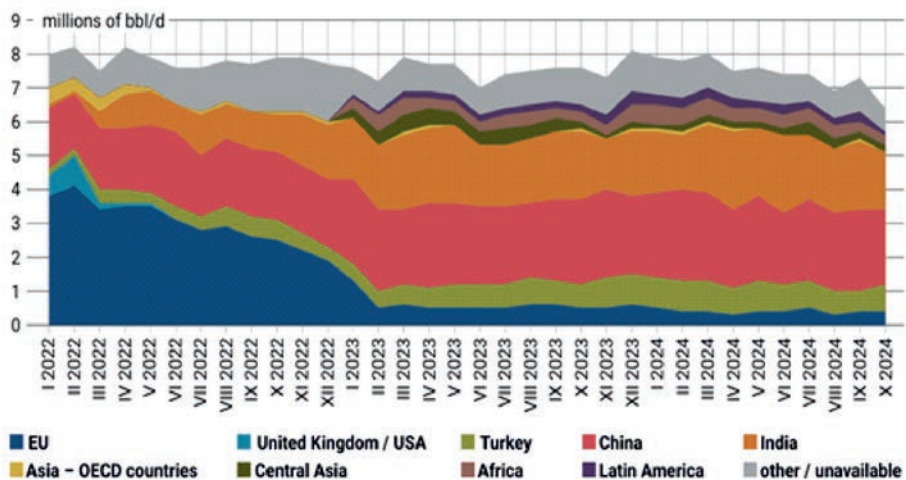
Another area that has been affected by international sanctions is the smartphone and laptop market, where in 2023 there was a decrease in the total value of imported devices by approximately 15%, revealing that cheaper and lower quality models were purchased. Thus, the smartphone market was dominated in 2023 by China, which held a 79% market share of the total. Samsung held a 10% share (approximately 3 million units), and Apple had an 8% market share (approximately 2.5 million units, a 50% decrease from 2021, although the total value decreased by only 30%). Analysis of the market has shown that Russian consumers tend to save money when purchasing electronic devices and to ensure access to maintenance and technical support services during the warranty and post-warranty periods, which is becoming increasingly difficult for Western brands. There is also a noticeable trend in the market towards the illegal import of counterfeit products, which account for approximately 30% of the market, with sales mainly taking place in online stores (Interfax RU, 2024).

The imposition of restrictions on the export of oil and petroleum products from Russia has affected not only that country, but also the global market. The energy sector (natural gas and oil) accounted for approximately 30% of the Russian Federation's total revenue, with most of it coming from exports of oil and oil derivatives. In 2021, Russia was the world's third largest oil producer, surpassed only by the USA and Saudi Arabia, but it was the largest exporter (prior to 2022, Russia's exports of oil and oil products accounted for 13% and 11% of global sales, respectively).

In this context, the restrictions imposed on the Russian Federation on exports of oil and petroleum products focused on two areas: imposing an embargo on these products at the level of the G7 member states and adopting a price cap mechanism

to reduce the Russian Federation's revenues. Thus, the maximum price was set at USD 60/barrel, and two quotas were imposed for fuels, namely products with a high profit margin (e.g. diesel, petrol) of approximately USD 100/barrel and products with a low profit margin (e.g. fuel, oil), for which the price was capped at USD 45/barrel. The purpose of the price cap was to avoid a sudden reduction in global oil supplies and a fall in the prices of Russian oil and petroleum products.

In order to effectively combat the restrictive measures imposed mainly by the EU on Russian oil imports, as well as the embargo imposed by the G7 countries, Russia has directed its exports of energy products (oil and natural gas) to other emerging markets. To understand the market share of Western countries, it should be noted that in 2021, before the outbreak of the conflict in Ukraine, Russia exported approximately 100 million tonnes of oil to the G7 countries and 76 million tonnes of oil to EU member states. Thus, oil purchases that were previously made by Western countries were taken over by two countries with great economic potential, namely China and India. Russia has thus become dependent on the two Asian countries, which have taken advantage of this aspect, by imposing low oil prices, leading to the economic development of China and India, which have access to energy resources at extremely competitive prices. According to Russian authorities' statistics, approximately 90% of oil exports went to these two countries. In terms of refined petroleum product exports, Russia has identified new customers in Asia, Africa and South America, thus diversifying its foreign market in order to withstand international sanctions imposed by Western countries.



Graph 2: Destinations of Russian Federation exports of oil and petroleum products between 2022 and October 2024 (International Energy Agency, authors' processing)

As can be seen in *graph 2*, the dependence of EU Member States on the Russian Federation's oil resources has fallen dramatically during the analysed period, highlighting the effectiveness of international sanctions against the authorities in Moscow.

To counteract the sanctions, Russia has set up a "*ghost fleet*" that transports Russian oil and fuel, thus defying the efforts of the Western coalition members. According to data provided by the Kiev School of Economics, this so-called "*ghost fleet*" has about 90 oil tankers. At the same time, unidentified buyers have purchased 187 second-hand oil tankers, including from European shipowners, for a total value of \$3.8 billion. In this context, it is assumed that a large part of these oil tankers are currently used by Russian shipowners to transport Russian oil products (Nightingale, 2023).

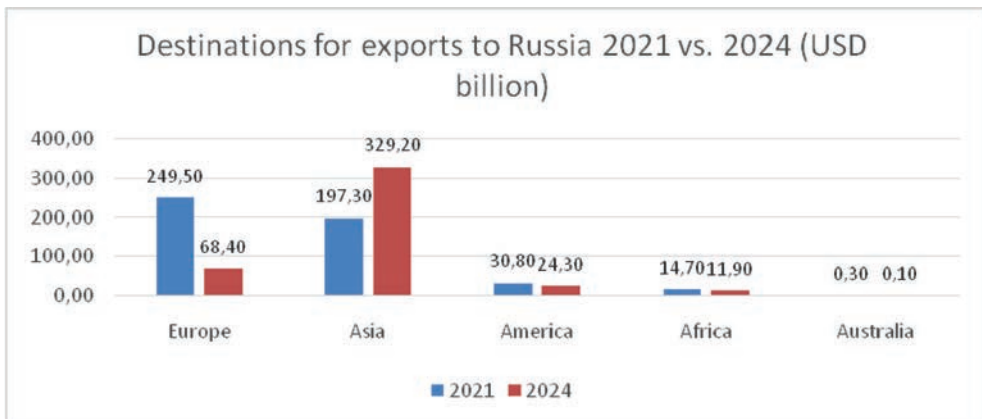
Another method used by Russian shipowners to transport petroleum products is to cooperate with Western entities (transport service providers, insurers, port authorities etc.) by providing transponders to transmit false location signals in order to conceal their connection with petroleum products of Russian origin. In addition, oil from the Urals region is mixed with other types of oil on board oil tankers to conceal its origin, which, according to the European Commission, constitutes a violation of the international sanction regime imposed on the Russian Federation (Wisniewska, 2023-2).

According to some estimates, in November 2024, approximately 34% of the oil and petroleum products exported by Russia by sea were transported using oil tankers owned or insured by Western companies, particularly European ones, compared to 80% before February 2022. At the same time, it is possible that some of these oil shipments violated the price cap.

In the case of exports of other raw materials (e.g. coal, diamonds, gold, timber, metals), Russian companies use intermediaries based in third countries. For example, before 2022, EU Member States were the second largest export market for Russian coal after China, receiving approximately 25% of Russia's coal exports. After the introduction of sanctions, coal imports into the EU fell to almost zero, forcing the Russian Federation to export coal to China, India and Turkey. However, through companies in Kazakhstan and Kyrgyzstan, covert coal exports to EU Member States, particularly Poland and Lithuania, continued. Kazakhstan increased its coal exports to the EU by approximately 29 times, from 56,000 tonnes in 2021 to over 1.6 million tonnes. The largest quantity of coal was exported to Poland (50% in 2022 and 60% in 2023). At the same time, the quantities exported by Kyrgyzstan to the EU were much smaller, namely 54,000 tonnes in 2023 (previously, this country did not export any coal).

As for gold exports, since 2022, Russia has been exporting to the United Arab Emirates, Hong Kong and Turkey, whereas before the attack on Ukraine, the Moscow authorities exported gold to the United Kingdom of Great Britain and Northern Ireland (beneficiary: London Bullion Market Association – LBMA). Starting in 2023, the export trend to these countries changed through the Eurasian Economic Union, particularly through Armenia. Thus, in the first half of 2024, Armenia imported 68 tonnes of gold from the Russian Federation worth USD 4 billion, compared to 17 tonnes and USD 1 billion in 2023 (Zayakin, 2024). This disproportionate import of gold by Armenia raises suspicions that the gold was exchanged for cash and securities in order to avoid using the banking system, so that there would be no electronic traces and the amounts obtained would not be confiscated by the authorities. This informal gold exchange system allowed the Russian Federation to obtain currency to finance the illegal war in Ukraine. Other countries involved in the illicit export of gold from the Russian Federation were Uzbekistan and Kazakhstan. Thus, in 2023, the United Kingdom of Great Britain and Northern Ireland imported 200 tonnes of gold from Kazakhstan and 40 tonnes from Uzbekistan, while Switzerland received 50 tonnes and 100 tonnes respectively.

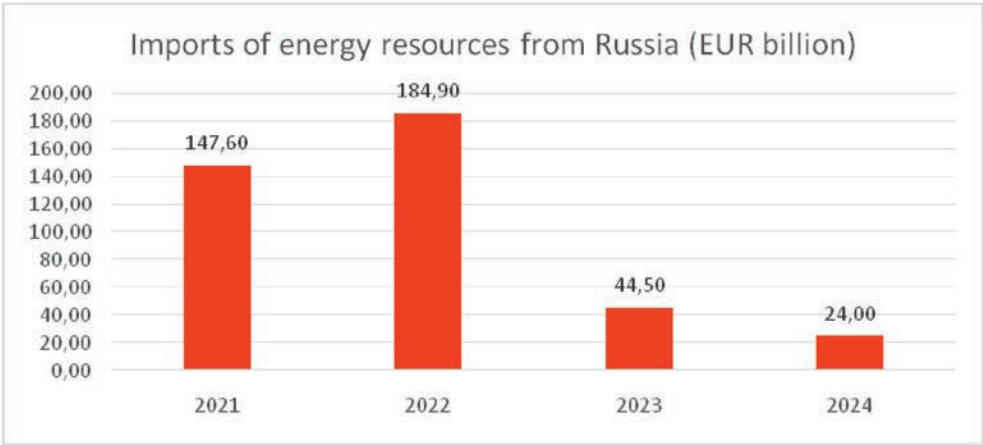
Armenia was also used as the main route for diamond exports to the United Arab Emirates, exporting 30 times more (4.5 million carats) than it actually produced. Diamond exports to India in 2024 increased by 22% compared to the same period in 2023, reaching 4.1 million carats (Collins, 2024).



Graph 3: Destinations of Russian goods exports 2021 vs. 2024
(Customs Service of the Russian Federation, authors' processing)

The analysis of *graph 3* clearly shows a substantial reduction in Russian exports to Europe and an exponential increase in exports to Asia, confirming the hypothesis that the Moscow authorities have identified new markets, particularly in China and India.

However, it is important to note that certain countries in Central and Eastern Europe, including Austria, the Czech Republic, Slovakia and Hungary, import energy resources (oil and natural gas) from the Russian Federation via pipelines, and certain countries in Western Europe (e.g. France, Italy, Belgium, Germany) continue to purchase LNG from Russia. Thus, the EU remains in fourth place in terms of energy resource purchases from Russia, paying EUR 24 billion in 2024, although the volume of these resources has decreased substantially compared to 2022 (Raghunandan, 2025). In order to further reduce the Russian Federation’s revenues, it is necessary to identify additional energy resources from countries that are not subject to sanctions and to carry out thorough and comprehensive checks to identify the origin of products in order to avoid imports of Russian energy products from countries that re-export them claiming they are from their own production.



Graph 4: EU imports of energy resources from the Russian Federation (EUR billion)
(Eurostat, authors’ processing)

The Russian Federation makes extensive use of cryptocurrencies for concealment and cross-border settlements to circumvent international sanctions. In 2023, Russia mined approximately 54,000 bitcoins, worth a total of USD 3 billion. In this context, the number of large farms and related infrastructure in the Russian Federation has increased significantly. The largest mining farm in Russia is located in Bryansk and is managed by BitRiver, a company linked to Russian oligarch Oleg Doripaska, who is on the international sanctions list (Savic, 2024).

MEASURES NEEDED TO STRENGTHEN THE SANCTIONS REGIME AGAINST THE RUSSIAN FEDERATION

Although successive packages of international sanctions have been imposed on the Russian Federation, their effects have been limited, given that the authorities in Moscow have identified certain vulnerabilities in Western states, which they have exploited opportunistically. In this context, Western states must focus on the strict application of sanctions and compliance with them. Thus, although the European Commission has presented its vision of desirable behaviour, it is not legally binding, and each EU Member State is free to interpret the expression “*all efforts*” differently. In this context, not all EU Member States currently recognise that violations of the sanction regime imposed by Western states on the Russian Federation constitute a criminal offence (Amberg, 2024).

It is also necessary for Western countries to monitor and comprehensively analyse, in particular, the Russian Federation’s neighbouring countries, which are used by the Russian authorities to export products subject to sanctions or to import products and technologies that can be used by the Russian military complex.

Another very important aspect is the identification of legal loopholes and the strengthening of legislation related to the implementation of international sanctions, given that Russian entities are quickly adapting to these sanctions. In this context, it is necessary to extend sanctions whenever necessary, while at the same time effectively combating measures taken by the Russian Federation to circumvent sanctions.

Harmonising the restrictions imposed on Russia and Belarus is essential, given that the two countries act in synergy, with the Republic of Belarus benefiting from political and economic support from the authorities in Moscow and the two countries coordinating their actions.

At the same time, it is necessary to achieve better cooperation and coordination of activities between national customs institutions and services and those of the European Commission and relevant European agencies (e.g. OLAF, FRONTEX). Close cooperation with the business sector is very important, and a clear communication policy is needed, including the creation of an online platform to collect all data on international sanctions and practical guidance on their implementation.

The diplomatic efforts of the EU and other states in their relations with third countries used by the Russian Federation to circumvent international sanctions must focus on convincing them of the need to apply international sanctions voluntarily in order to avoid prolonging the military conflict in Ukraine. An example in this context is the US policy which, through diplomatic pressure on certain

third countries threatened with secondary sanctions, has discouraged companies in those countries from conducting commercial operations with the Russian Federation.

CONCLUSIONS

Although the sanctions regime imposed by the Western community on the Russian Federation is consistent, this state continues to use deceptive methods to circumvent it, making it necessary to take firm action to identify the entities that benefit from these practices and to sanction them accordingly. At the same time, diplomatic pressure must be intensified on third countries that support the Russian Federation in circumventing international sanctions, and Western companies that support these illegal mechanisms must be directly sanctioned.

One aspect of great importance is the complete withdrawal of EU Member States from the process of purchasing energy resources from the Russian Federation, including the elimination of derogations for Central and Eastern European countries that allow purchases through the Druzhba pipeline, as well as the introduction of an embargo on imports of piped natural gas and liquefied natural gas (LNG) from the Russian Federation.

At the same time, there must be a further reduction in EU cooperation with the Russian Federation in the field of nuclear energy and a complete severing of ties (there are 19 nuclear reactors built with Russian technology operating in the EU).

Finally, it is necessary to explore new innovative ways to target the Russian economy, including regulating certain restrictions on Russian companies' access to the EU market through the intelligent use of the tariff regime. With regard to sanctions targeting the Russian financial sector, it is necessary to disconnect a significant number of Russian banks from the SWIFT system, increase the number of sanctioned banking institutions, introduce sanctions for other financial institutions (e.g. the Moscow Stock Exchange), requiring European financial institutions (e.g. Raiffeisen Bank, UniCredit, OTP Bank) to withdraw from the Russian market, and imposing EU restrictions on banks in third countries that support the Russian Federation in processing transactions that are subject to the sanctions regime.

BIBLIOGRAPHY:

1. Amberg, P. (2024). *EU Russia and Belarus sanctions: New guidance on "best efforts" obligations and reminder on introduction of enhanced due diligence obligations*, Global Sanctions and Export Controls Blog, 26.11.2024, sanctionsnews.bakermckenzie.com, retrieved on 16 September 2025.

2. Chupilkin, M., Javorcik, B., Plekhanov A., *The Eurasian roundabout: Trade flows into Russia through the Caucasus and Central Asia*, EBRD Working Paper no. 276, European Bank for Reconstruction and Development, February 2023, ebrd.com, retrieved on 15 September 2025.
3. Collins, S. (2024), *Russian diamond shipments to India up 22% in 1H*, Eurasia Business News, 02.09.2024, eurasiabusinessnews.com, retrieved on 16 September 2025.
4. European Commission (2022). Preventing Russian Export Control and Sanction Evasion: Updated Guidance for Industry, https://finance.ec.europa.eu/document/download/ae2e63e2-4c4d-4f77-9757-c408ddbced1_en?filename=240924-preventing-russian-export-control-sanctions-evasion%20.pdf retrieved on 11 September 2025.
5. European Commission (2024). *List of Common High Priority Items* (Version of February 2024), finance.ec.europa.eu, retrieved on 13 September 2025.
6. Cook, C., Seddon, M. (2023). *The shadowy network smuggling European microchips into Russia*, Financial Times, 12.11.2023, ft.com, retrieved on 15 September 2025.
7. Eurasian Economic Commission (2022). *Zero rates of import customs duties on components for handheld power tools to be extended for one year*, <https://eec.eaeunion.org/en/news/nulevye-stavki-vvoznykh-tamozhennykh-poshlin-na-komplektuyushchie-dlya-ruchnykh-elektroinstrumentov/>, retrieved on 14 September 2025.
8. Interfax RU (2024). *În Rusia crește piața gri a smartphone-urilor*, <https://www.finmarket.ru/main/article/6294771>, retrieved on 16 September 2025
9. Kłysiński, K., Matuszak, S. (2024). *Dynamic imports vs. dwindling exports. Belarus–EU trade in 2023*, OSW, 11.03.2024, osw.waw.pl, retrieved on 15 September 2025.
10. Kommersant (2024). *Великий тернистый путь, Коммерсантъ*, 20 august 2024, www.kommersant.ru/doc/6905203, retrieved on 15 September 2025.
11. Michalski, A., Wisniewska, I. (2023). *Turkey: the transit of goods subject to Western sanctions face restrictions*, OSW, 15.03.2023, osw.waw.pl, retrieved on 15 September 2025.
12. Nightingale, A., Lee, J., Cho, S. (2023). *How an Aging Armada and Mystery Traders Keep Russian Oil Afloat*, 12.05.2023, bloomberg.com, retrieved on 16 September 2025.
13. ONU (2022). *Aggression against Ukraine: resolution/adopted by the General Assembly*, 02.03.2022, <https://digitallibrary.un.org/record/3959039>, retrieved on 11 September 2025.
14. Pierzchala, B. (2024). *Finding Our Bearings: Tracking Circumvention of EU Dual-Use Sanctions to Russia*, OSW data spotlight, osw.waw.pl/sanctions, retrieved on 15 September 2025.
15. Raghunandan, V., Katinas, P. (2025). *December 2024 – Monthly analysis of Russian fossil fuel exports and sanctions*, Centre for Research on Energy and Clean Air (CREA), 10.01.2025, energyandcleanair.org, retrieved on 16 September 2025.
16. Rudnik, F. (2024). *The effects of the sanctions: the Russian LNG sector's problems*, OSW Commentary, no. 578, 07.03.2024, osw.waw.pl, retrieved on 16 September 2025.

17. Savic, B. (2024). *Russia's digital assets challenge Western sanctions*, Geopolitical Intelligence Services, 21.11.2024, gisreportsonline.com, retrieved on 16 September 2025.
18. Simola, H. (2023). *Latest developments in Russian imports of sanctioned technology products*, BOFIT Policy Brief 2023, no. 15, 29.11.2023, publications.bof.fi, retrieved on 15 September 2025.
19. SIPRI (2025). *SIPRI Arms Transfers Database*, Stockholm International Peace Research Institute, sipri.org, retrieved on 15 September 2025.
20. Tkachova, A. (2024). *Sanctions against Russia: The Coalition Can Do Better— for Ukraine and Global Order*, Just Security, 23.04.2024, justsecurity.org, retrieved on 15 September 2025.
21. Verstka Media (2025). *We Can Help and Deliver: Who Imports Sanctioned Aircraft into Russia*, <https://verstka.media/we-can-help-and-deliver-who-imports-sanctioned-aircraft-into-russia>, retrieved on 16 September 2025.
22. Zayakin, A., Ergnyan, S. (2024). *Golden intrigues. How Russia circumvents sanctions by exporting billions of dollars' worth of gold through Armenia*, *The Insider*, 22.11.2024, <https://theins.ru/en>, retrieved on 16 September 2025.
23. Yle News (2023). *Luxury car smugglers bypass Russian sanctions via Finland*, Yle News, 02.10.2023, yle.fi, retrieved on 15 September 2025.
24. Wisniewska, I. (2023-1). *The silence of the lambs. Russian big business in wartime*, OSW Commentary no. 503, 28 March 2023, osw.waw.pl, retrieved on 13 September 2025.
25. Wisniewska, I. (2023-2). *Tightening restrictions: the EU's eleventh package of sanctions against Russia*, OSW, 26.06.2023, osw.waw.pl, retrieved on 16 September 2025.

THE COGNITIVE COMPONENT OF THE RUSSIAN FEDERATION'S WAR AGAINST UKRAINE

Lieutenant Georgiana BLĂJAN

Psychological Operations Center "Samoilă Mârza", Bucharest

DOI: 10.55535/RMT.2025.3.21

The global competition among major powers is taking on new dimensions in the context of technological evolution, particularly with the emergence of new forms of conflict. The war between the Russian Federation and Ukraine marks a transformation in modern warfare, highlighting the use of methods specific to cognitive warfare, in which information technologies, artificial intelligence, and media channels are employed to influence the perceptions, behaviors, and societal cohesion of the civilian population. Russia has made extensive use of such tools to shape specific narratives, induce confusion, and undermine Ukraine's informational resilience. This article aims to provide a perspective on the importance of the information space as a new strategic battlefield, illustrating specific practices of the Russian Federation's cognitive warfare in Ukraine.

Keywords: cognitive warfare; artificial intelligence; war in Ukraine; media literacy; cognitive superiority;

INTRODUCTION

Concerns regarding the cognitive component of warfare, viewed in NATO's doctrine for information operations as a dimension of the information environment, have increased significantly in recent years, particularly due to the difficulty of identifying specific threats. With the development of propaganda tools employed by the Russian Federation against the West, the North Atlantic Alliance has placed greater emphasis on the need to achieve cognitive advantage, which has led to the conceptualization of the term "*cognitive warfare*" (adopted in Romanian as "*război cognitiv*") (NATO Cognitive Warfare Concept, 2025).

Although controversies have existed, either regarding the similarity of this concept to other related notions or concerning the challenges of defining it as a distinct domain or dimension, the importance of its application is indisputable, especially in the context of technological advances in artificial intelligence and innovations in cognitive sciences. These aspects are considered fundamental for leveraging this dimension on a much broader scale.

Currently, the most relevant example of the application of cognitive warfare can be found in the conflict in Ukraine, where the Russian Federation has made extensive use of this type of warfare to influence not only the perceptions of the Ukrainian population but also international public opinion. The leadership in Moscow benefits from long-standing experience in this field, frequently being cited in discussions on information manipulation and media control. Thus, through elaborate disinformation campaigns, manipulation of the information environment, and strict control of internal information flows, Russia has sought to erode trust in Ukrainian institutions and to divide society. This strategy was intended to compensate for certain deficiencies in conventional military capabilities, by providing a strategic advantage through influencing the adversary's decisions and behaviors. Moreover, the use of advanced technologies, such as artificial intelligence and digital platforms, has amplified the impact of these actions.

Taking the above into consideration, this article proposes an analysis of the evolution of the concepts underlying the term "*cognitive warfare*", culminating in an examination of the application of cognitive warfare in Russia's strategy against Ukraine. Finally, the article outlines future development perspectives of the cognitive

warfare concept, highlighting not only its strategic and technological implications in current and future conflicts, but also the associated ethical dimensions, as well as the need to enhance societal resilience in the face of this type of threat.

THEORETICAL APPROACHES TO THE CONCEPT OF COGNITIVE WARFARE

The term “*cognitive warfare*” has been the subject of significant debate in the specialized literature, either due to its perceived similarities with other pre-existing forms of conflict or because of the variable interpretations of the proposed definitions, which did not indicate substantial conceptual evolution beyond earlier theoretical frameworks. Nevertheless, the use of specific instruments by certain actors to shape the information environment for their own purposes, combined with the exponential development of technology, has generated the need to address such a concept. In order to outline a comprehensive and nuanced understanding of cognitive warfare, this section analyzes a series of relevant definitions from the specialized literature.

The Russian Federation’s Perspective

The Russian Federation possesses one of the oldest and most consolidated traditions in the use of psychological influence instruments, disinformation, and strategic manipulation, with roots that long predate the emergence of modern concepts of cognitive warfare. In this context, Russian military doctrine can be analyzed over time through several key concepts, such as *Maskirovka*, *Active Measures*, *Reflexive Control*, and *New Generation Warfare*. Although each of these notions has distinct characteristics, they are linked through doctrinal continuity, representing successive stages in refining the way Russia conceives and conducts influence operations and indirect conflict.

The term *Maskirovka*, often inadequately translated as “*camouflage*”, represents the traditional foundation of Russian military deception in the twentieth century. The concept dates back to 1904, with the establishment of the first specialized school, the Higher School of Studies (Bouwmeester, 2017). A more concrete explanation of military deception refers to the use of “*the complex of measures devised to confuse the enemy regarding the presence and disposition of forces, their condition, readiness, actions and plans*” (Bechis, 2020, p. 122). Although historically similar measures can be identified as far back as antiquity

(Sun Tzu's philosophy – *"All warfare is based on deception"*), the adaptation of *Maskirovka* covered a much broader scope, aiming at *"rational manipulation, either through the dissemination of contradictory information or by supporting false conclusions."* (Anuța, 2016, p. 45). The method reached its peak during the Second World War, through the success achieved against German troops; a result later explained (Don Levine, 1960 apud Zimmer, 2013) by the fact that *"the government was essentially a counterintelligence apparatus. It was conceived in 1903 by Lenin as an operation in counterintelligence against the Czarist regime, and it remained a conspiracy ever since"*, suggesting that Russian ideology has long been closely tied to practices of disinformation and information control, whose scale significantly exceeded the capabilities of other actors.

The *Active Measures Program* (in Russian, *Aktivnye Meropriyatiya*) was intended to go well beyond the previous concept, being carried out primarily by state structures (intelligence services, government agencies) in order to achieve strategic objectives without resorting to military force. The dating of the term is relatively vague, but it is generally accepted that the Union of Soviet Socialist Republics (USSR) used it beginning in the late 1950s to describe a set of covert and deniable operations of political influence or subversion. These included (but were not limited to) the establishment of front organizations, support for allied political movements, the orchestration of internal unrest, and the dissemination of disinformation (Galeotti, 2019). According to the same author, the concept was described in the *Counterintelligence Dictionary* (1972) of the KGB's *"Felix Dzerzhinsky"* Higher School as being used in counterintelligence activities by state security organs, encompassing projects aimed at strengthening the position of spies within and near the enemy camp, targeted disinformation actions against the adversary, compromise and demoralization operations, the transfer to USSR territory of individuals with special operational value, the acquisition of information of strategic interest, and similar activities.

The theory of *Reflexive Control (RC)* is the concept most frequently encountered in the specialized literature when discussing the introduction of the domain of *"cognitive warfare"* in connection with the Russian Federation. First formulated in the Soviet Union in the 1960s by Vladimir Lefebvre, it attracted interest within Soviet military circles and was formally adopted by the Soviet Army only in the late 1970s. Reflexive Control is most often examined as *"a mechanism for influencing the decision-making process of a state and involves the transmission of fabricated*

information (partially true, partially false) to the adversary in order to induce it to make a voluntary decision favorable to the initiator's interests" (*Reflexive Control Theory in the Logic of Hybrid Warfare*, 2017). Consequently, Reflexive Control is considered an important component in the evolution of Russian doctrine, as it goes beyond the tactical and operational levels associated with *Maskirovka*, having a strategic impact during the Cold War.

The most up-to-date approach to the use of manipulation at the strategic level is the so-called *Gerasimov Doctrine*, derived from an article written in 2013 by Russian General Valery Gerasimov, Chief of the General Staff of the Armed Forces of the Russian Federation, translated into English as *"The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations"*. The author's vision referred to the blurring of the line between war and peace, as well as to the fact that *"the focus of applied methods of conflict has altered in the direction of the broad use of political, economic, informational, humanitarian, and other nonmilitary measures – applied in coordination with the protest potential of the population."* (Gerasimov, 2013, p. 1). This description further intensified the interest of the Russian Federation in applying non-kinetic instruments to achieve cognitive advantage.

Ultimately, the concepts practiced by Russia in association with cognitive warfare are not an innovation of the Putin era, but rather a strategy with deep historical roots. Nevertheless, under his leadership, forms of influence have been refined and applied on a large scale, with the introduction of a new key instrument – the civilian population – increasingly used as a means of shaping the information environment.

The Interdisciplinary Approach

The notion of *cognitive warfare* has been adopted both in military and academic literature, with multiple experts becoming aware of how technology has been used to influence the evolution of certain trends across various states.

The cognitive component was studied several decades ago, during the analysis of the USSR's success in applying Reflexive Control. Specialized literature (Chotikul, 1986, p. 43) noted that *"cognition results from the reflection of the material world in the human mind"*, which explains why Soviet doctrine focused on influencing environmental conditions in order to constrain the enemy to act accordingly.

Beginning in 2019, the concept was adopted by several authors who specifically associated it with its exploitation by the Russian Federation or China, emphasizing

that it represents *“a strategy that focuses on altering how a target population thinks – and through that how it acts”* (Backes, Swab, 2019 apud Deppe, Schaal, 2024). A more comprehensive definition describes cognitive warfare as *“an unconventional form of warfare that uses cybertools to alter enemy cognitive processes, exploit mental biases or reflexivethinking, and provoke thought distortions, influence decision-making andhinder actions, with negative effects, both at the individual and collective levels”* (Bernard, Cluzel, 2020, p. 2). This definition introduces technology as a key vector for transmitting manipulative messages.

NATO's Conceptualization

The first NATO member to invoke the term *“cognitive warfare”* was the United States of America (2017), with the aim of describing the means available to an actor to manipulate the cognitive mechanisms of an enemy or a population in order to weaken, penetrate, influence, or even subjugate or destroy it (Ib.).

Within NATO, the term was officially institutionalized and promoted starting in 2020 by the NATO Innovation Hub, through a series of strategic reports defining cognitive warfare as an advanced form of conflict that targets not only information control, but also the cognitive processes of individuals – perceptions, emotions, memory, and decision-making capacity. The development of a common concept within the Alliance became necessary as a result of hostile actions conducted in the sphere of cognitive warfare against member states; therefore, representatives of the academic community and analytical centers were also integrated into the process of establishing the conceptual framework.

According to the *NATO Cognitive Warfare Concept* (2025, p. 5), the term is defined as *“the fight for cognitive superiority. Contesting in this environment comprises deliberate, synchronized military and non-military activities throughout thecontinuum of competition designed to gain, maintain and protect cognitive advantage”*. The document also highlights the relevance of cognitive warfare through the development of technologies such as the militarization of nanotechnologies, biotechnologies, and human augmentation, suggesting that the configuration of future conflicts will no longer belong exclusively to the informational domain.

China's Perspective

Chinese strategists identified the value of the cognitive domain as early as the early 2000s. In recent years, China has devoted increased attention to the potential use of neuroscience and artificial intelligence, not only in the medical field, but also in the development of cutting-edge advanced technologies.

The *China Brain Project* (CBP) regained priority in 2021, despite having been postponed for five years due to ethical concerns regarding its application (Normile, 2022). Guo Yunfei (President of the Information Engineering University under the Strategic Support Force of the People's Liberation Army) argued that *"among the physical, informational, and cognitive domains, the cognitive domain will ultimately become the primary battlefield of military confrontation between major powers. Warfare in the cognitive environment directly affects the brain, influencing emotions, motivations, judgments, and actions – and may even control the enemy's brain."* (*The Future of China's Cognitive Warfare: Lessons from the War in Ukraine*, 2020).

Conceptual Deconfliction

The innovative character of the term and the absence of a dedicated doctrine often leave room for interpretations or overlaps between cognitive warfare and other notions such as *psychological operations* (PsyOps) or *information warfare*.

Unlike PsyOps, which are used exclusively in the military domain and directed at a specific target audience, cognitive warfare proposes a broader approach that integrates PsyOps tactics but is not limited to them. Thus, cognitive conflict employs multiple instruments of power, supplemented by emerging technologies, neuroscience, and digital platforms, in order to control the behavior of large groups of individuals.

With regard to information warfare, NATO approaches it from the perspective of protecting access to sensitive information, intercepting and exploiting the adversary's information, destroying information infrastructures, and disrupting communication flows. Cognitive warfare, by contrast, expands the field of action, focusing not only on data or communication channels, but on how individuals perceive, process, and respond to information. Complementarily, the *NATO Cognitive Warfare Concept* (p. 4) states that the term *"should also not be misconstrued as StratCom by another name. InfoOps, PsyOps, and MilPA are only some of the capabilities and functions used in the daily contest for cognitive advantage"*.

THE INSTRUMENTALIZATION OF COGNITIVE WARFARE IN RUSSIA'S STRATEGY AGAINST UKRAINE

The Russian Federation's experience in employing forms associated with cognitive warfare is deeply rooted in the history of its relations with Western states, but especially in maintaining control over territories within the former Soviet space. Although the Putin regime was not the first to embrace expansionist visions

centered on disinformation and the manipulation of reality in order to distort behavior, upon his accession to the presidency, the focus shifted toward controlling information and the ways in which it reaches citizens, specifically to serve regime interests. Such actions were initially directed at Russia's own population, with the Kremlin introducing new forms of information control on an annual basis starting in 2000. At present, any expression perceived as contradicting the Kremlin's agenda is subject to punishment, with censorship intensifying following the launch of the full-scale invasion of Ukraine (Bugayova, Stepanenko, 2025). Regarding the conduct of the war in Ukraine (2022), Russia has effectively employed a range of instruments associated with the cognitive component in order to compensate for gaps in conventional capabilities, making clear that the successes achieved would not have been possible through military means alone. To provide a more comprehensive picture of the behavioral influence ecosystem used by the Russian Federation against Ukraine, the evolution of this mechanism is analyzed both in the pre-conflict phase and after the outbreak of hostilities.

Before 2022: Preparing the Information Terrain

Ukraine's orientation in the early 2000s toward transparent, Western-inspired governance was perceived by the Russian central authorities as a direct threat to the Putin regime. Consequently, Moscow intensified its external cognitive warfare efforts by launching information campaigns designed to undermine democratic processes and slow Ukraine's rapprochement with the West. Following the Orange Revolution, which resulted in the rerun of presidential elections and the appointment of a pro-European candidate despite Putin's preferred contender, Russia began constructing and disseminating narratives of separatism in Ukraine. These narratives were later strategically activated in 2014 during the hybrid operation to occupy eastern and southern regions of the country (Bugayova, Stepanenko, 2025). They were further reinforced by messaging that emerged in the aftermath of the Euromaidan protests (autumn 2013), with Russian media portraying the demonstrations as *"an unconstitutional coup endangering the Russian-speaking population"* (Hofirek, 2021, p. 11).

The effects included the organization of anti-Euromaidan protests from Odesa to the Luhansk regions and Crimea, ultimately culminating in the annexation of Crimea and the outbreak of the conflict in Donbas. The use of proxy groups (through protesters) and disinformation elements (via conspiratorial narratives such as the alleged abandonment of Ukraine – and implicitly Crimea – by the West;

the historical and spiritual unity between Ukraine and the Russian Federation; and Russia's role as protector of abandoned states) aimed to foster among audiences in the affected regions the belief that annexation did not constitute aggression, but rather a historical restoration (Chiriac, 2021). Although the strategies employed in Crimea and Donbas were similar, the outcomes differed due to *"the lack of Russian regular forces' timely decisive action (which) caused the conflict to transform into a frozen conflict"* (Hofirek, p. 2).

Following the military interventions of 2014, Russia recalibrated its national security paradigm, culminating in the adoption of the new Information Security Doctrine (December 2016). The document reflected a strongly defensive vision, portraying Russia as a *"besieged cyber fortress"*. It emphasized threats originating from foreign states – ranging from cyberattacks and digital espionage to ideological influence – while advocating stronger internal control over the Russian internet, reduced dependence on Western technologies, and the development of domestic IT capabilities (Pynnöniemi, Kari, 2016). Framing Russia as a victim of Western attacks served to justify the malign intentions the Kremlin intended to pursue.

Moreover, in the same year, Putin approved the Foreign Policy Concept of the Russian Federation, which reinforced the objective of *"strengthening the position of Russian media and communication outlets in the global information space and conveying Russia's perspective on international processes to a broader international audience"*. Over the past decade, Moscow has relied on multiple channels to disseminate Russian propaganda internationally, including multilingual state-backed media outlets (RT, Sputnik, and TASS) as well as proxy websites (News Front, SouthFront, Geopolitica.ru, Strategic Culture Foundation), which, although not officially acknowledged by the Russian state, are indirectly controlled by it (Romanian Intelligence Service, 2020). State-controlled media entities have received substantial funding to broadcast Kremlin-favorable messaging in multiple languages and regions worldwide. The objective was **to construct a parallel reality** in which the West is depicted as morally declining, contrasted with an image of Russia as a defender of traditional values, sovereignty, and an *"authentic"* global order. Another key element of the strategy involved **delegitimizing Western media and cultivating informational ambiguity** aimed at eroding the public's ability to distinguish between truth and disinformation, ultimately leading to the demoralization of civilian populations regarding the credibility of information disseminated by official authorities.

Between 2014 and 2022, Russia continued to test and refine instruments associated with cognitive warfare. Among the measures employed were: (1) **plausible deniability**, through which Russia rejected direct involvement in the Donbas conflict, attributing actions to “volunteers” or “local forces”; (2) **informational fog**, created by the deliberate dissemination of contradictory versions of events; and (3) **influence campaigns** conducted in the West, used to test cognitive manipulation techniques later applied in the Ukrainian context. This period marked the transition from fragmented actions to a coherent strategy in which the cognitive component became essential to achieving the Russian Federation’s geopolitical objectives.

The 2022 Invasion: Escalation of Cognitive Warfare

Russia employed cognitive warfare instruments to facilitate the war in Ukraine, such that in the days preceding the invasion, President Putin and Russian-affiliated media outlets consistently disseminated reassuring messages asserting that Russia had no intention of invading Ukraine - while, in reality, final preparations were being made for Russian forces to cross the border and occupy large portions of Ukrainian territory (Burke, Henschkel, 2022).

Another example of a cognitive attack explored in the prelude to the conflict (NATO Cognitive Warfare, June 2025, p. 6) was the dissemination of the narrative concerning the “13 biological laboratories in Ukraine”, suggesting that the United States was transforming Ukraine into a testing ground for biological weapons with the approval of the Ukrainian president. The Kremlin strategically amplified this narrative through platforms such as RT, Telegram, and other social media networks, using manipulated documents and distorted information to target international audiences, particularly in regions where skepticism toward Western institutions already existed. According to the NATO document, the campaign was designed to exploit cognitive biases such as distrust toward U.S. foreign policy and fear of biological threats – heightened in the aftermath of the COVID-19 pandemic – with the ultimate aim of undermining trust in the United States and NATO, justifying Russian aggression as a defensive measure, and creating confusion regarding the true nature of the conflict. The intended effect was not physical, but psychological: shaping perceptions, redirecting blame, and weakening international resolve.

The outbreak of the conflict itself was framed by the Russian president under the label of a “special military operation”, justified as an act of “denazification” of Ukraine and later as “a struggle for the future, for the freedom of countries and peoples” (Putin, 2023). The intensive use of messaging centered on the term

“Nazism” expanded its meaning to such an extent that it was incorporated into the latest version of the Foreign Policy Concept of the Russian Federation (2023), alongside other key terms such as *“Western hegemony”*, *“neo-colonialism”*, *“the collective West”*, and *“Russophobia”* in legitimizing the evolution of the war in Ukraine.

The dissemination of propagandistic messages through media channels – both within Ukraine and in other states supporting the Ukrainian side – was conducted in parallel with Moscow’s investments in building a transnational network of pro-Russian journalists and influencers. This effort involved training programs, media partnerships, and the transfer of ideological *“know-how”* (Center for Countering Disinformation, 2025). Ultimately, this process formed part of a broader strategy aimed at imposing Russian narratives globally, implemented through both traditional media channels and digital platforms, social networks, online influencers, and coordinated disinformation campaigns.

The manner in which Moscow employed technology to propagate disinformation represented a novel element in the conduct of modern conflicts. The use of bots (computer programs operated within bot farms that generate targeted content for or against specific topics), trolls (individuals using false identities to disseminate propagandistic content), and artificial intelligence (a field of computer science focused on creating systems capable of mimicking human intelligence) significantly amplified the impact of messages on citizens’ cognitive processes. The terms *“bot”* and *“troll”* are often incorrectly used interchangeably, yet their modes of operation differ: bots can rapidly disseminate messages at scale, while trolls intervene strategically to stimulate conflict, manipulate conversations, and lend credibility to disinformation. Maximum effectiveness – also leveraged by the Kremlin – is achieved when these tools are combined, creating the illusion of authentic consensus and amplifying the impact of desired narratives.

Their use was evident from the early stages of the conflict, with Ukrainian special services identifying over one and a half million accounts across various social networks and messaging platforms (...) *“created to spread falsehoods and pro-Russian propaganda”* (Ministry of Internal Affairs of Ukraine, December 2022). Bot and troll networks remain a persistent method of shaping the conflict, despite multiple countermeasures undertaken by security services and social media platforms. Their impact on influencing mass behavior is considerable, given that most individuals are not accustomed to verifying the authenticity of information and that attribution is difficult to establish. Furthermore, their proliferation

in the information environment has increased due to the exploitation of artificial intelligence, whose increasingly sophisticated outputs are difficult to challenge even by domain experts.

As noted by F. Bechis in *Playing the Russian Disinformation Game* (p. 125), social media platforms have fundamentally reconfigured propaganda campaigns previously employed, granting states the ability to target adversaries in ways that were previously inconceivable. These platforms enable access to vast audiences within informal settings, embedded directly in users' everyday environments, thereby increasing the effectiveness of transmitted messages. Moreover, campaigns conducted through social media are difficult to detect and counter, requiring significantly fewer financial resources than conventional methods of psychological or kinetic influence.

These characteristics prompted the Kremlin to allocate substantial resources to the development of a coherent and advanced digital disinformation strategy. Unlike many Western states, Russia stands out for the scale and depth of its influence programs, which integrally mobilize state, media, and technological resources in a concerted effort of cognitive influence and information manipulation.

The dissemination of Russia's own perspectives through various overt and covert means, combined with the exploitation of **existing social, economic, and political cleavages** within target states, has supported Moscow's objectives of undermining international solidarity with Ukraine and instilling among the Ukrainian public the belief that Russia plays the role of a victim vis-à-vis the West and that of a liberator of Ukraine.

PERSPECTIVES

Although Russia has not fully achieved its objectives in Ukraine, the use of instruments specific to the cognitive component of warfare has intensified in recent years, and their effects are increasingly evident. Within the information environment, concerns have grown regarding potential innovations that Russia may adopt in the future. These concerns also extend to the expanding cooperation between Moscow and Beijing, with the latter being widely recognized for its significant technological advances.

Another aspect requiring further examination in the near future is media literacy as a means of enhancing cognitive resilience. The cognitive warfare conducted by Russia in Ukraine and other areas of interest should serve as a lesson learned for strengthening interinstitutional cooperation, while also engaging

multiple audience groups as an integral part of total defense (Solvita, 2022). In an information environment saturated with increasingly sophisticated cognitive influence campaigns, the active promotion of media literacy is not merely an educational necessity, but a vital strategy for national security and regional stability. Consequently, encouraging sustained citizen engagement and education in this field represents a fundamental pillar in effectively responding to the challenges posed by the cognitive component of conflict.

Approaching the conflict in Ukraine from the perspective of cognitive warfare on a global scale also entails questioning the ethics of this type of conflict, as it influences people's thinking and decision-making without their awareness. In a context where the boundary between peace and war is becoming increasingly blurred, and confrontations are often conducted within the cognitive domain, the effects on civilian populations can be profound and long-lasting. For this reason, security specialists must be prepared not only to identify and counter such threats, but also to manage the increasingly complex ethical challenges raised by the evolving nature of contemporary conflicts (Rusu, 2025).

CONCLUSIONS

The Russian Federation is widely recognized for its extensive experience in the field of information manipulation. While its official rhetoric has remained consistent – portraying Russia as a victim of Western actions while simultaneously maintaining expansionist ambitions – the country has become a relevant example of the transition from classical propaganda to the integration of modern technologies in shaping mass behavior.

The conflict in Ukraine has been accompanied by an unprecedented intensification of cognitive warfare conducted by the Russian Federation, directly targeting the manipulation of perceptions and the disruption of the cognitive coherence of both the Ukrainian population and the international public. Through a combination of official narratives, disinformation campaigns, the use of affiliated media channels, influencers, and automated networks (bots and trolls), Russia has promoted themes such as Ukraine as a failed state, the “Nazification” of Ukrainian society, the historical legitimacy of territorial annexation, and the attribution of blame to NATO and the West for the outbreak of the conflict.

Cognitive warfare has also expanded into European states, aiming to divide public opinion and weaken political support for Ukraine. As a result, the cognitive domain has become an essential battlefield in which Russia has invested strategic

resources, anticipating that informational victory may precede or even substitute for military success.

Against the backdrop of the intensification Russia's cognitive warfare efforts, NATO and Western states have become increasingly concerned with developing defensive capabilities within the information environment. In this context, NATO has explicitly acknowledged in recent strategic documents the importance of protecting the "cognitive space" of its citizens. Moreover, media literacy campaigns are becoming essential for strengthening societal resilience, as Russian cognitive interventions can undermine democracy from within, even in the absence of a conventional conflict.

BIBLIOGRAPHICAL REFERENCES:

1. Anuța, C. (2016). *Old and New in Hybrid Warfare. Countering Hybrid Threats: Lessons Learned from Ukraine*.
2. Bechis, F. (2020). *Playing the Russian Disinformation Game Information operations from Soviet tactics to Putin's sharp power*. Democracy and Fake News.
3. Claverie, B., Cluzel F. (2020). *The Cognitive Warfare Concept*.
4. Bouwmeester, H. (2017). *Lo and Behold: Let the Truth Be Told –Russian Deception Warfare in Crimea and Ukraine and the Return of 'Maskirovka' and 'Reflexive Control Theory'*, în *Netherlands Annual Review of Military Studies*.
5. Bugayova, N. (2025). *A Primer on Russian Cognitive Warfare*, Institute for the Study of War, <https://understandingwar.org/research/cognitive-warfare/a-primer-on-russian-cognitive-warfare/>, retrieved on 23 September 2025.
6. Burke, P., Henschke, A. (2022). *I Know My Truth... Now Tell Me Yours: From Active Measures To Cognitive Warfare In The Russian Invasion Of Ukraine*. Strategic Panorama.
7. Center for Countering Disinformation (2025). *How Russia Spreads Its Propaganda Worldwide Under the Guise of Education*, <https://cpd.gov.ua/en/international-threats-en/europe/how-russia-spreads-its-propaganda-worldwide-under-the-guise-of-education/>, retrieved on 23 September 2025.
8. Chiriac, O. (2021). *Cognitive Warfare in the 21st Century Great Power Competition – Framing of Military Activity in the Black Sea, Romanian Military Thinking International Scientific Conference Proceedings*, 3rd III.
9. Chotikul, D. (1986). *The Soviet Theory of Reflexive Control in Historical and Psychocultural Perspective: A Preliminary Study*. Naval Postgraduate School.
10. Deppe, C., Schaal, G-S. (2024). *Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory concept*, <https://www.frontiersin.org/journals/big-data/articles/10.3389/fdata.2024.1452129/full>, retrieved on 22 August 2025.
11. Embassy of the Russian Federation in Romania (2023). *Vladimir Putin: "Operațiunea Militară Specială este o luptă pentru viitor, libertatea țărilor și a popoarelor"*, <https://>

- romania.mid.ru/ro/press-centre/arkhiv_novostey/vladimit_putin_opera_iunea_militar_special_este_o_lupt_pentru_viitor_libertatea_rilor_i_a_popoarelor/, retrieved on 25 September 2025.
12. Galeotti, M. (2019). *Active Measures: Russia's Covert Geopolitical Operations*, <https://www.marshallcenter.org/en/publications/security-insights/active-measures-russias-covert-geopolitical-operations-0>, retrieved on 23 September 2025.
 13. Gherasimov, V. (2016). *The Value of Science Is in the Foresight New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operation*, în *Military Review*, The Professional Journal Of The U.S. Army.
 14. Hofirek, M. (2021). *Messing with their Minds: Maskirovka's Cognitive Effects in Crimea and Donbas*.
 15. Morelle, M. et al. (2023). *Towards a Definition of Cognitive Warfare. Conference on Artificial Intelligence for Defense*, p. 3.
 16. NATO Cognitive Warfare Concept (2025). Version 1.3.
 17. Normile, D. (2022). *China bets big on brain research with massive cash infusion and openness to monkey studies*, <https://www.science.org/content/article/china-bets-big-brain-research-massive-cash-infusion-and-openness-monkey-studies>, retrieved on 23 September 2025.
 18. Pynnöniemi, K., Kari, M. (2016). *Russia's New Information Security Doctrine: Guarding a besieged cyber fortress*. Finnish Institute of International Affairs.
 19. Rusu, A. (2025). *Military ethics in the light of Cognitive Warfare*. International Conference RCIC`25, p. 49.
 20. Serviciul Român de Informații (2020). *Tehnici de propagandă rusă*. Centrul de Excelență OSINT.
 21. Solvita, D-L. (2022). *With Media Literacy Towards Cognitive Resilience: Updates from the Baltic States, and lessons learned*.
 22. *Teoria controlului reflexiv în logica războiului hibrid* (2017), <https://intelligence.sri.ro/teoria-controlului-reflexiv-logica-razboiului-hibrid/>, retrieved on 23 September 2025.
 23. *The Future of China's Cognitive Warfare: Lessons from the War in Ukraine* (2020), <https://warontherocks.com/2022/07/the-future-of-chinas-cognitive-warfare-lessons-from-the-war-in-ukraine>, retrieved on 24 September 2025.
 24. The Ministry of Foreign Affairs of the Russian Federation (2016), *Foreign Policy Concept of the Russian Federation*, /efaidnbmnnnibpcajpcgclefindmkaj/[https://www.russiamatters.org/sites/default/files/media/files/Foreign%20Policy%20Concept%20of%20the%20Russian%20Federation%20\(approved%20by%20President%20of%20the%20Russian%20Federation%20Vladimir%20Putin%20on%20November%2030,%202016\)%20-%20Asset%20Publisher%20-%20The%20Ministry%20of%20Foreign%20Affairs%20of%20the%20Russian%20Federation.pdf](https://www.russiamatters.org/sites/default/files/media/files/Foreign%20Policy%20Concept%20of%20the%20Russian%20Federation%20(approved%20by%20President%20of%20the%20Russian%20Federation%20Vladimir%20Putin%20on%20November%2030,%202016)%20-%20Asset%20Publisher%20-%20The%20Ministry%20of%20Foreign%20Affairs%20of%20the%20Russian%20Federation.pdf), retrieved on 24 September 2025.

25. The Ministry of Foreign Affairs of the Russian Federation (2023), *Foreign Policy Concept of the Russian Federation*, https://www.mid.ru/en/foreign_policy/fundamental_documents/1860586/, retrieved on 24 September 2025.
26. Zimmer, P. (2013). *Maskirovka: The Hidden Key to Soviet Victory*, Warfare History Network, <https://warfarehistorynetwork.com/article/maskirovka-the-hidden-key-to-soviet-victory/>, retrieved on 23 September 2025.

DEMOGRAPHY AS AN ELEMENT THAT INFLUENCES NATIONAL POWER

Major General (ret.) Associate Professor Dr. Grudi ANGELOV

Colonel (ret.) Professor Dr. Stoyan STOYCHEV

University of Library Studies and Information Technologies, Sofia, Bulgaria

DOI: 10.55535/RMT.2025.3.22

In the present paper, the authors examine demography, as an element of the social factor within the framework of NATO's comprehensive approach. On this basis, they set themselves the goal of revealing its influence on the national and allied power of a given country or alliance. The emphasis is on the importance and influence of the demographic element, an invariable part of the social factor, and its impact on the maintenance of national and allied power. The methodology used by the authors includes a systematic approach – suitable for the study of interconnected and related activities. The implementation of the chosen methodology has been achieved using literature review, comparisons, system analysis, theoretical research, and military scientific analysis. The paper is intended to be a logical attempt to reveal the significance and influence of demography on the essence of the social factor as an indispensable part of national power and national security.

Keywords: comprehensive approach; demography; social factor; national power; security;

INTRODUCTION

In the contemporary world, we are witnessing unprecedented transformations in the security environment, driven by and resulting from globalization, dynamic social processes, and growing interdependence among states. Within this context, *demography is emerging as a key factor with direct and long-term implications for the national power and security* of modern states. It constitutes an integral part of the social dimension within NATO's comprehensive approach and occupies a central position in the analysis of resilience, development, and strategic capabilities of any given nation. The comprehensive approach is a key principle of the Alliance, which underlies the preparation and conduct of every NATO operation, campaign or non-combat action (Stoychev, 2023, p. 8).

Demographic trends – such as population aging, declining birth rates, migration processes, and the associated socio-economic transformations – have a direct impact on a state's capacity to sustain its national power, both independently and within allied frameworks.

In the modern world, national power is determined not only by a country's economic and military capabilities but also by a complex set of social, political, cultural, and technological factors. Among them, *demography occupies a particularly important place*. The population represents the bearer of social capital, the primary source of labour, military potential, and political legitimacy (Nye, 2004, p. 45). In this context, demographic processes are not only a quantitative dimension but also a strategic factor, which determines the long-term trajectory of development for every state.

The development of national power requires a systematic approach that integrates the demographic dimensions with economic, political, and military factors. That is precisely why many contemporary researchers emphasize the link between demographic trends and the ability of states to defend their interests in the international system (Kugler, 1989).

Historical experience shows that demography is one of the most reliable indicators of the rise and fall of states and empires. A classic example is the Roman Empire, whose demographic decline is associated with the weakening of its military capacity and economic base (Goldstone, 2012).

Similar processes can also be observed in the Ottoman Empire, where the decline of the productive population and internal migration weakened state stability. In contemporary terms, examples such as Japan and Germany illustrate how aging populations and low birth rates pose serious challenges to social systems, defence capacity, and economic resilience (Coleman, 2006).

Conversely, India and Nigeria demonstrate the potential of young and numerous populations to drive economic growth and enhance international influence. In this sense, demography is established as a structural component of the social factor, which occupies a central place in comprehensive models of national power. It influences all other elements – economic, military, political, and cultural.

The present paper aims to analyse the role and significance of demography as an element of national power, to present the main challenges and their impact on security and economy, as well as to propose conceptual models for assessing and integrating demographic factors into strategic planning.

The methodology of the present study is based on a systematic approach, which enables the analysis of the interrelations among various elements of national power. Methods of analysis and synthesis, system decomposition and aggregation, as well as comparative analysis of existing models have been applied. Both theoretical studies and a military science perspective have been used to highlight the importance of demographic factors for the defence capabilities of the state. Such an interdisciplinary approach ensures the objectivity, complexity, and reliability of the conclusions drawn (Bloom, 2003).

A key emphasis is placed on the relationship between demography and national security. Negative demographic trends – such as population decline, aging, and migration – can weaken social stability, increase pressure on social systems, and limit defence capacity. In contrast, positive demographic trends create conditions for economic growth, innovation, and the expansion of strategic capabilities.

According to Grudi Angelov *“without a stable demographic structure, national strategies remain fragile, as there is insufficient human potential to achieve the national goals and to guarantee sovereignty”* (Angelov, 2024a). Particular importance is attached to examining the demographic factor in both international and allied contexts. Within organizations such as NATO and the EU, demographic differences among member states affect their ability to contribute to collective security. Countries with negative population growth face challenges in providing military and economic support, while states with young and growing populations may play an increasingly significant role in allied strategies (EU Commission, 2020).

Alongside the mentioned aspects, demographic processes have a direct impact on economic development. The labour force is not only a resource for production but also a determining factor for innovation and competitiveness. Therefore, investments in education and healthcare as well as a sound migration policy become tools for offsetting negative demographic trends (Bank, 2019). This is where the role of strategic planning and the need for a long-term national doctrine become evident, by integrating demographic priorities into the overall development framework of the state (Angelov, 2024b).

The scholarly relevance of the topic stems from the fact that, under conditions of global uncertainty, demography becomes a key indicator of resilience. As Nye points out, national power is no longer defined solely by military and economic dimensions, but also by the state's ability to manage social capital and human resources (Nye, 2004). That is precisely why the systematic study of demographic factors is a prerequisite for the creation of effective strategies and policies that ensure national security and prosperity.

This study investigates the influence of demography on the structure and projection of national power with particular attention to its integration into strategic policy development. The following key objectives are set:

- To examine demography as a structural component of the social factor as well as in relation to national security;
- To analyse demographic challenges and their impact on economic and defence development;
- To present existing models for assessing national power and to propose a conceptual model integrating demographic indicators.

This study is intended to contribute both to the theoretical debate on national power and security and to the practical application of strategic planning. In this regard, it follows the logic of contemporary works in the field, which highlight the need for a systemic and comprehensive approach in examining the relationship between demography and national power.

On the other hand, this study seeks to contribute to the scholarly discourse on national power and security by providing a focused examination of the demographic dimension as a strategic variable. It builds upon recent academic developments that advocate for an integrated, multidisciplinary approach to understanding how demographic dynamics shape a state's long-term capacity and influence. By adopting a research-driven perspective, the study emphasizes the need for robust analytical frameworks that connect population trends with national strategic objectives.

DEMOGRAPHY AS A STRATEGIC DETERMINANT OF NATIONAL POWER

In the context of globalization, migration processes, increasing labour mobility, and technological change, demography has become one of the key parameters for strategic planning. Over the past decades, a number of countries with aging populations have faced the need to adapt their defence and social systems to new realities. At the same time, countries with young and growing populations are encountering challenges related to unemployment, social instability, and migration pressure.

Demography is not merely a statistical indicator, but a strategic factor that directly influences the formation and development of national power. In classical theories of international relations, national power is often associated primarily with economic strength and military capabilities (Morgenthau, 1948). In the contemporary context, however, social dimensions – including demography – are gaining increasing importance, as human capital is a fundamental resource for sustaining resilient institutions, driving innovation, and ensuring national security (Nye, 2004). As Grudi Angelov emphasizes *“population dynamics is not only a background variable, but a direct determinant of the strategic capacity of the state”* (Angelov, 2024a, p. 122). It suggests that demographic trends play a fundamental role in shaping national strategy and doctrine, as well as in the development of models for assessing national power.

On the other hand, the strategic or so-called environmental factors, encompassing the political, economic, military, social, informational, and infrastructural systems, are deeply interwoven and mutually influenced by demographic characteristics. Therefore, demographics characteristics are directly influenced by the determination and the supporting elements of the national power.

Even a cursory review, or a preliminary study of these factors, reveals the extent of their interdependence and impact. For example:

- ❖ *Political factors/systems* concern the stability of a state, coalition, or alliance; governance and public administration; the functioning of judicial institutions; law, order, and legitimacy; the dynamics between groups with converging or opposing political interests; and the conduct of international relations and diplomacy;

- ❖ *Military factors/systems* encompass issues of security, stability, and threat environments – both internal and external; the armed forces, their readiness, manning, and sustainment (where demographic characteristics play a critical role); internal security forces; paramilitary and irregular formations (again shaped by societal demographics); as well as armaments, equipment, and logistics;

❖ *Economic factors/systems* relate to vital national resources and critical infrastructure (including human resources), production, markets and trade, the distribution of goods and services, consumption, inflation, debt, and other aspects of national economic resilience;

❖ *Infrastructural factors/systems* address energy, transportation nodes and networks, communications infrastructure, industry, and public facilities;

❖ *Informational factors/systems* involve national intelligence, mass communications and media, the information activities of societal groups, susceptibility to manipulation and disinformation, vulnerabilities to messaging, and the resilience of established information and communication systems.

❖ *Social factors/systems* include social support structures, healthcare, education, quality of life, human development, advocacy and pressure groups, displaced persons, and refugees – all of which, as noted, being also integral to the demographic profile of a population or society.

These strategic factors are inseparably linked to the instruments of national and allied power that states or coalitions of states develop and maintain across the continuum of contemporary strategic competition. This continuum encompasses both peaceful competition or rivalry and the phase of cooperation. Within this framework, NATO identifies four primary instruments of power: diplomatic, informational, military, and economic (DIME model).

Demography as a Structural Component of the Social Factor

Demographic characteristics – such as population size, age structure, migration patterns, educational profile, and urbanization – form the foundation of a country's social capital. These features have a direct impact on economic development, political stability and defence capabilities.

❖ *Population size* – a large population provides a greater pool of human resources for both economic and military activities. China and India are examples of countries leveraging their demographic potential to gain global influence. Conversely, smaller states often compensate for limited population size through innovation and participation in international alliances (Singer, 1985);

❖ *Age structure* – a youthful population serves as a driver of economic growth, whereas an aging population presents significant challenges to social systems and defence readiness (Coleman, 2006). Europe, for instance, faces demographic aging that limits its labour force and increases public spending on social services;

❖ *Total Fertility Rate (TFR)* – the average number of children a hypothetical cohort of women would have at the end of their reproductive period if they were subject during their whole lives to the fertility rates of a given period and if they were not subject to mortality. It is expressed as children per woman;

❖ *Migration* – the emigration of young and skilled individuals weakens national potential. However, well-managed immigration can strengthen the economy and support societal development (Bank, 2019);

❖ *Educational profile* – an educated population enhances national competitiveness and increases innovation capacity. In this regard, investments in education are viewed as strategic investments in national power (Bloom, 2003);

❖ *Urbanization* – the population concentration in urban centres facilitates economic dynamism and innovation, but it also raises the risk of social tensions and inequality.

These strategic factors are inseparably linked to the instruments of national and allied power that states – or coalitions of states – develop and maintain across the continuum of contemporary strategic competition.

The Link between Demography and National Security

Demographic processes have a direct impact on national security. They influence both social stability and defence capabilities.

❖ *Social stability* – negative demographic trends – such as low birth rates, population aging, and migration pressure – can undermine public trust in institutions and generate internal tensions (Teitelbaum, 1985);

❖ *Defence capabilities* – conscription pool, along with health and educational levels, are key determinants of military readiness. In the context of demographic decline, the state is often forced to rely on high-tech systems or allied support (Angelov, 2024a);

❖ *External threats* – demographic vulnerability may expose a country to external pressures – such as migration crises, demographic spill from neighbouring states, or subversive activities by hostile actors.

In his presentation at the 45th International Congress of Military History, Grudi Angelov pointed out that: *“Without a stable demographic structure, the national strategy remains fragile, as there is no sufficient human potential to achieve the national goals and to guarantee sovereignty”* (Angelov, 2019). This conclusion aligns with international scholars that underscore the role of demography as a fundamental component of national security.

Demography and Economic Development

Demographic dynamics plays a crucial role in shaping economic outcomes and therefore human capital represents the primary resource for production, innovation and consumption. The labour force is a key driver of economic growth, while the population age structure determines not only the supply of labour market but also the demand for goods and services across different sectors. In this context, countries with young and growing populations often benefit from the so-called “*demographic dividend*” – a period during which the share of the working-age population is significantly higher than that of the dependent population (children and the elderly). It creates favourable conditions for economic expansion, if it is accompanied by adequate education, healthcare and economic policies. A classic example of such positive dynamics is India, where the youthful age structure supports both domestic consumption and the global supply of labour (Bloom, Canning, 2003). When properly managed, these demographic characteristics become a strategic advantage that can sustain long-term economic growth and strengthen the country’s position in the international system.

Demographic trends have a profound and direct impact on national economic performance and strategic capacity. One of the most pressing negative developments is population aging, which leads to an increase in social expenditures and a decline in the available labour force-factors, which poses significant challenges to economic stability and growth. Japan serves as a classic example of such demographic transition, where a rapidly aging population has placed considerable strain on the welfare system and contributed to long-term stagnation in productivity and economic output (Coleman, 2006, p. 53). In contrast, proactive strategies such as well-regulated immigration policies and sustained investments in education have the potential to mitigate these adverse effects. By replenishing the workforce and enhancing human capital, such measures not only support economic resilience but also reinforce the broader dimensions of national power (Bank, 2019). Therefore, adapting to demographic shifts through comprehensive and forward-looking policy frameworks is essential for maintaining socioeconomic stability and strategic autonomy in the context of global competition and internal transformation.

Demography and Strategic Planning

In the context of modern strategic governance, demography must be regarded not merely as a background variable but as a central and dynamic component of national power. Strategic planning and the formulation of national strategies and doctrines require the integration of demographic indicators in order to provide a realistic and sustainable basis for decision-making. Population size, structure,

distribution, and trends influence a state's capacity to generate economic output, maintain security, support innovation, and ensure social cohesion, which are core elements of long-term strategic effectiveness.

Without integrating demographic analysis, national strategies risk overlooking critical vulnerabilities or untapped potentials. As Grudi Angelov argues, strategic documents such as the National Security Strategy or National Doctrine remain incomplete and potentially ineffective if they do not explicitly account for population dynamics (Angelov, 2024a, p. 163). It is particularly evident in the formulation of defence policies, labour force development, education systems, healthcare planning, and migration management, all of which are interdependent with demographic trends.

Recent approaches to measuring national power increasingly incorporate demographic variables alongside traditional indicators such as economic strength, military capability, political stability, and technological advancement (Ib., p. 122). These integrated models adopt a system-based perspective, recognizing population dynamics not merely as static background data but as active multipliers of a state's strategic capacity. For instance, a young and well-educated population can enhance a country's ability to innovate, compete globally, and maintain national resilience. Conversely, a rapidly aging population lacking sufficient social infrastructure may impose significant burdens on the economy and weaken the long-term sustainability of public policy and national defence.

Furthermore, the development of a comprehensive *Grand Strategy* – a long-term, all-encompassing vision that aligns a nation's objectives with its available resources and capacities – must be grounded in a thorough understanding of demographic realities. Demography shapes the scope and limits of the state actions, both domestically and internationally. It determines the sustainability of public policy, the resilience of institutions, and the credibility of national commitments in alliances and international organizations such as NATO or the EU. In this regard, demographic research becomes not merely a statistical exercise but a cornerstone of strategic foresight and governance.

DEMOGRAPHIC CHALLENGES AND THEIR IMPACT ON NATIONAL POWER

Demographic processes are not static phenomena, but dynamic social factors that shape a state's capacity to build and sustain its national power. In the context of global security and international relations, they have become a critical indicator of societal resilience, economic development, and defence capabilities (Bloom, Canning, 2003; Coleman, 2006).

An analysis of demographic challenges reveals that they can have both internal dimensions – affecting social stability and institutional resilience – and external ones, related to the state's international influence and its obligations within allied frameworks. Without systematic consideration of demographic risks, national strategies are in danger of losing their relevance and applicability in real-world security contexts (Angelov, 2019, p. 88).

On this basis, we will present some fundamental dependencies and influences of this element – demography, in relation to national power. The authors of the present paper, even without referring to the so-called “*demographic wars*”, have every reason to assert their position now: in just 30 years, the world will be unrecognizable. Unrecognizable because, according to them, demographic parameters not only influence, but are fundamentally at the core of the social factor, of the generation and maintenance of national power. From there, the connection to the outcome of the confrontation in contemporary global politics – which we have been witnessing for over a decade – is direct.

We can boldly state that this aspect of global rivalry is still underestimated. Yet, it is precisely that aspect (*demography*) that will ultimately determine the results of the transformation of the global community: the transition from a unipolar to a multipolar world, a transition that is already underway (and will be completed no later than the end of the 2030s). Not artificial intelligence (despite all its significance), not smartphone factories, but demography will decide everything. Moreover, the ideas that will be instilled in the minds of future generations. But for now, let us talk about demography.

Demographic Decline and National Security

Negative demographic trends – declining birth rates, population aging, and high levels of emigration – have a direct impact on national security.

❖ *Population aging* is a phenomenon that leads to a decrease in mobilization potential and an increase in social expenditures. Countries such as Japan and Italy are experiencing difficulties in maintaining their defence capabilities precisely due to demographic aging (Coleman, 2006);

❖ *Emigration*, defined by the mass departure of young and educated individuals, weakens the economy and limits the potential for military modernization. In some countries, this process is described as a “*brain drain*”, which undermines strategic resilience (Bank, 2019);

❖ *Social cohesion* or lack thereof witnesses the weakening of social trust, which can lead to political instability and increased vulnerability to external influences (Teitelbaum, 1985, p. 112).

National security is inseparable from the demographic base of society, as without it, no defence system can sustain itself in the end (Angelov, 2019). This observation is particularly relevant for small states, whose limited material and technological resources make them especially reliant on the quality and availability of their human capital. In such contexts, demographic trends such as population decline, brain drain, and aging can have a disproportionately large impact on national resilience, economic competitiveness, and defence capabilities. Therefore, maintaining a stable and productive demographic base is not merely a social priority, but a strategic imperative for ensuring national sustainability and sovereignty in a highly interconnected global environment.

Continuing the exploration of the demographic element, the authors of the paper focus on another illustrative (not only according to them) example of how direct and immediate the connection is between building and maintaining a nation's power and how the demographic decline can impact the national security. The example concerns Sweden and Israel, and we can pose the question: Which country continues to build its national power and national security, and which one fails to maintain them?

When discussing demographic policy – or policies aimed at the demographic element of a given country – examples are often brought up highlighting how important financial well-being is when having a child, as well as the various measures of social support for families with children.

So, what is the situation, or what are the important living and reproductive conditions for the population in Sweden?

In Sweden, people live in comfort and prosperity from a purely financial point of view. There is no need to worry about becoming homeless, elderly people are not abandoned, and every child is guaranteed a place in kindergarten. Sweden is a country well-known, not just in Europe, for its social policy. And this is for good reason: the core lies in the fact that Sweden implements a consistent demographic policy aimed at genuine care – not only for the elderly, but also for children and for the families in which these children are born.

Yet, despite all these favourable conditions and policies that support the demographic element, in 2023 Sweden recorded the lowest birth rate in its entire history – since such records and statistics have been kept, essentially since the 18th century. The fertility rate dropped in that year to 1.45 children per woman

– well below the so-called replacement level, which is generally accepted as 2.1 children per woman of childbearing age. In fact, this places Sweden among the lowest in Europe.

A rhetorical question arises naturally: Why, despite all the mentioned advantages, does no woman in Sweden want to give birth?

The answer according to the authors, and not just them, is this: comfort does not automatically produce offspring. Offspring is about trust. It is continuity. It is the sense that there is something greater than one, something one is called to serve.

In Sweden, there is no such purpose. There is no nation as an idea. There is no religion to justify sacrifice. There is no military duty, no historical pain, no memory for which someone would be willing to die – and therefore live – for something greater than themselves. Personal well-being and individual success are present. Collective ones, however, have dissolved.

On the other side is Israel. A country that for decades has been in a state of emergency, of tension, of mobilization, and of war. Where every morning can begin with a siren, and every summer with a new campaign in the Gaza Strip (not only as now, with one of the largest-scale campaigns there). But the fertility rate there is 2.9 – the highest among developed countries. And in this case, it is not just a statistic, it is a diagnosis. And in that diagnosis lies everything: economy, culture, faith, fear, national power, and purpose.

Israel is an anxious country. But it knows who it is. It knows where it came from and where it is going. There, family and the continuation of lineage are not an *“option”* or a *“choice”*, but a duty to the ancestors and a matter of survival. There, a child is not an *“extra expense”*, but a participant in a common cause. Yes, the State of Israel pays for childbirth. It covers in vitro fertilization (IVF). It supports mothers. But that is not the main thing – Sweden has those policies too. The main thing is in the minds of the people, of the population, of society. In Israel, even so-called secular women have three or four children. Because society expects it. Because family is the centre of society, not a personal project or personal interest.

In Israel, meaning, honour, duty, and participation – for every citizen, not only for the woman who gives life – are not something belonging to the past. They are the present itself, the present upon which Israel builds its future, and with which it builds and sustains its national power. If we are to describe in another way the demographic element in Israel, we can say that in the entire society there is a clear understanding: the woman continues, the man carries, and the child receives. And all of this is called Kin.

Demography, however, is not only about characteristics and social policies – it is a matter of national security. It is not just one of the topics, even if we call that topic “*national power*”. First and foremost, it is a matter of survival. But we know that a state can survive and move forward in time with a clearly built and sustained, strong – not hollow or imaginary – national power.

In the provided examples of Sweden and Israel, it is telling how, because of misguided, unclear, or poorly presented policies in the sphere of demography and in the social, cultural, and economic factors, a country like Sweden demonstrates how a nation in comfort heads toward its decline, and perhaps even toward gradual assimilation and oblivion. Israel, on the other hand, shows how a nation in a state of anxiety gives a meaning to birth. How it not only builds but sustains its national power, how it moves forward to defend its national interests, even though compared to Sweden, it (the State of Israel) is surrounded almost entirely by hostile countries.

Impact on Defence Capacity

Military power is traditionally regarded as a core element of national strength. However, the quality and quantity of the human resources it depends on are intrinsically linked to demographic processes.

- ❖ Shortage of military personnel. Countries experiencing population decline face difficulties in recruiting sufficient numbers of military personnel. It necessitates changes in military structures and a shift toward professional armed forces and reserves (Singer, Bremer, Stuckey, 1972).

- ❖ Technological compensation. When human resources are limited, states often invest in high-tech weaponry and defence systems. However, it requires substantial financial resources that not all countries can afford (Nye, 2004);

- ❖ Allied mechanisms. Smaller states frequently rely on collective defence within NATO and the EU to offset their demographic weaknesses (European Commission, 2022);

Based upon everything mentioned above, it could be outlined: “*For small states, demographic decline is not only a social problem, but also a defence problem, which requires reliance on alliances and shared security frameworks*” (Angelov, 2024a, p. 67).

The demographic characteristics of a country also influence the methods of confrontation and warfare that it is compelled to adopt when faced with the need to defend or uphold its national interests. For example, based on their demographic characteristics, a number of countries choose so-called asymmetric methods and actions as means of confrontation. In the contemporary context, we can also say

that hybrid actions or hybrid warfare represent such an asymmetric method – though not exclusively for countries with smaller demographic capacity or a smaller population. Of course, the concept of hybrid warfare is not a new discovery for modern society. It is a natural evolution of war (Yordanova, 2024).

Strategic Approaches to Demographic Challenges

Addressing demographic problems requires a comprehensive strategic approach that integrates economic, social, and defence policies.

- ❖ *Encouraging birth rates* – Tax incentives, social programs, and support for families can help mitigate the effects of low birth rates;

- ❖ *Managed migration* – Controlled immigration, combined with effective integration policies, can support the economy and renew the labour force.

- ❖ *Investments in education and healthcare* – Enhancing the quality of human capital is a key factor in societal resilience.

- ❖ *Adapting defence systems* – Incorporating reserve forces, modernizing the military, and integration into allied structures are all vital.

Taking everything mentioned above into account, it could be concluded that: *“The future of national power lies in the ability of states to adapt their strategies to demographic realities, rather than ignoring them”* (Angelov, 2024a, p. 140).

Overall, it could be summarized that, demographic challenges represent a fundamental factor influencing the economic development, social stability, defence capacity, and international role of states. Furthermore, negative trends – such as declining birth rates, population aging, and migration – require strategic approaches and international cooperation. Only by integrating demographic factors into national strategic planning can states build sustainable and effective national power.

CONCLUSIONS

In conclusion, demography is now widely acknowledged as a core determinant of national power, shaping and reinforcing its economic, social, military and political dimensions. The findings of this paper indicate that population should not be viewed solely through numerical indicators such as size or growth, but rather as a multidimensional factor reflecting the quality of human capital, the resilience of society, and the strategic capacity of the state to sustain long-term stability and advancement.

Chapter one clarifies the role of demography as a structural component of the social factor. The interdependence between age structure, educational profile, and geographic distribution of the population, on the one hand, and economic viability and defence capacity, on the other hand, have been highlighted. It has been

emphasized that demographic trends have direct implications for national security, as population aging and migration can weaken social cohesion and create strategic risks (Nye, 2004; United Nations, 2022).

Chapter two depicts the major challenges arising from negative demographic trends. They manifest both internally – through shrinking workforce, increasing social inequality, and decreasing mobilization potential – and externally – by reducing a state’s international influence and its contribution to collective security systems. Special attention has been given to the sustainability of social systems and the need for long-term policies aimed at encouraging birth rates, reducing emigration, and integrating migrants (Bloom, Canning, 2003; Coleman, 2006).

The synthesis of the examined issues leads to several key conclusions:

1. *Demography is a strategic resource* that shapes a state’s capacity for economic growth, defence sustainability, and social stability;
2. *Negative demographic trends* – such as population aging, low birth rates and emigration – pose a critical risk by undermining national resilience and reducing a state’s international influence;
3. *Strategic planning* necessitates the integration of demographic factors, as their absence renders national strategies and doctrines incomplete and challenging to implement;
4. The *international and allied context* amplifies the importance of demography, as demographic deficits in a single member state – within frameworks like NATO and the EU – can weaken overall collective security;
5. A *comprehensive approach* is essential, requiring demographic policies that include fertility incentives, strategies to encourage return migration, effective migrant integration, and sustained investments in education and healthcare.

As emphasized in recent literature, “*the integration of demographic indicators into a national power index is not optional but mandatory for states facing existential demographic risks*” (Angelov, 2024a, p. 112). Therefore, the strategic future of every nation – regardless of its size or economic strength – depends directly on its ability to manage and shape demographic dynamics.

In conclusion, demography should not be regarded as a secondary statistical variable but rather as a strategic pillar of national power and security. It reflects the current state of society and serves as a crucial indicator of its future trajectory. States that integrate demographic factors into their strategic frameworks will be better positioned to ensure stability, resilience, and international relevance in the face of global challenges.

BIBLIOGRAPHY:

1. Angelov, G. (2019). *The Treaty of Neuilly and its impact on the national power of Bulgaria*. Sofia: Public Policy.bg. doi:<https://doi.org/10.58894/EJPP.2020.2.349>.
2. Angelov, G. (2024a). *For (un)success of the nation and whether national doctrine and strategy are guarantee for country's prosperity*. Sofia: "За буквите – О писменехъ". doi:ISBN 978-619-185-664-0.
3. Angelov, G. (2024b). *State and Statehood: Etymology and Characteristics*. Saarbruken, Germany: Lambert Academic Publisher. doi:ISBN 978-620-780-614-0
4. Bank, W. (15 March 2019). *World Development Report 2019*. Washington DC, USA. doi:<http://doi.org/10.1596/978-1-4648-1328-3>.
5. Bloom, D., Canning, D. (2003). *The demographic dividend: A new perspective on the economic consequences of population change*. Santa Monica, CA, USA: RAND Corporation. doi:ISBN-13: 978-0-8330-2926-3.
6. Coleman, D. (September 2006). *Immigration and etic change in low-fertility countries: A third demographic transition*. *Population and Development Review*, 32, 52-96. doi:<https://doi.org/10.1111/j.1728-4457.2006.00111.x>.
7. European Commission (17 June 2020). *The impact of demographic change*. Brussels, Belgium, EU, https://commission.europa.eu/system/files/2020-06/demography_report_2020_n.pdf?utm_source=chatgpt.com, retrieved on 17 September 2025.
8. European Commission (2022). *European Commission Report of Demographic Change*. Brussels: EU Commission, https://commission.europa.eu/system/files/2020-06/demography_report_2020_n.pdf?utm_source=chatgpt.com, retrieved on 17 September 2025.
9. Goldstone, J. A. (16 August 2012). *Political demography: How population changes are reshaping international security and national politics*. p. 336. doi: ISBN: 978-0199945962.
10. Kugler, J. (1 September 1989). The power transition: A retrospective and prospective evaluation. Midlarsky, M. (ed.) *Handbook of War Studies*, pp. 171-194. ISBN: 9780044453411.
11. Morgenthau, H. J. (1948). *Politics among nations: The struggle for power and peace*. New York: Alfred A. Knopf. doi: ISBN: 978-0075544692
12. Nye, J. (11 May 2004). Soft power: The means to success in world politics. *Public Affairs*, p. 208. ISBN 978-158-648-306-7.
13. Singer, J. B. (1985). *Peace, War, and Numbers*. Beverly Hills: Sage. doi: ISBN: 978-0803901643.
14. Stoychev, S. (2023). *Joint operations and their planning*. Sofia, Bulgaria: "Dio Mira" Publishing House.
15. Teitelbaum, M. W. (1985). *The Fear of Population Decline*. Orlando, Florida, USA: Academic Press.
16. United Nations (2022). *World Population Report Prospects 2022*. New York: UN, https://www.un.org/development/desa/pd/sites/www.un.org.development.desa.pd/files/wpp2022_summary_of_results.pdf, retrieved on 17 September 2025.
17. Yordanova, S. (2024). *Techniques and Technologies of Non-Classical Wars*. Sofia: "За буквите – О писменехъ".

SILENT INVADERS: THE GROWING THREAT OF DRONES AND BALLOONS

Assistant Professor Dr. Adriana SAULIUC

Faculty of Educational Sciences Communication and International Relations,
"Titu Maiorescu" University; Senior Researcher,
Center for Conflict Prevention&EarlyWarning, Bucharest

DOI: 10.55535/RMT.2025.3.23

The use of drones and balloons as tools of hybrid warfare has become a reality in recent years that has complicated the security equation in Europe and especially on the Eastern Flank. The threat generated by the use of aerostats and drones in a pernicious manner seems to become an essential component of contemporary confrontation strategies. And this preference for these low-cost and operationally flexible technologies allows states and non-state actors to carry out actions that are difficult to attribute to hybrid aggressors, thus increasing strategic ambiguity. Drones facilitate smuggling, surveillance, intelligence gathering, and targeted attacks, while balloons can serve as monitoring platforms and as a means to test the limits of adversary airspace. Together, they expand the spectrum of unconventional tactics, altering the balance between offense and defense and complicating deterrence mechanisms. This article examines how these systems are reshaping the dynamics of modern conflicts, highlighting their security implications.

Keywords: drones; aerostats; hybrid warfare; hybrid threats; European Union;

INTRODUCTION

If discussions regarding drones are generally more recent, meaning the last few decades, as a result of their emergence, those regarding the use of balloons, whether we are referring to gas or hot air balloons, should take us back in time to long-gone periods, meaning several centuries ago.

Each of the two elements fits perfectly into the civilian dimensions of human activities, from leisure, to aerial filming of cultural, sporting and personal events, to mapping and use in agriculture, or in various fields, such as construction, civil emergencies, etc., and these are just a few of the actions that these types of aerial vehicles can perform. In general, balloons can be used for aerial photography, surveillance and monitoring, meteorological actions, and emergencies involving certain categories of disasters, while drones focus on largely the same aspects of entertainment, meteorology, search and rescue actions, etc.

Analyzing the various actions for which balloons and drones can be used, we identify a wide range of advantages that arise from their use, which inevitably led to the proliferation of these types of aircraft. A proliferation that over time has also seen an expansion of their use in the military field, an evolution that has also occurred as a result of the possibility of using drones in particular in a manner that is more than opportune for international state actors who have been concerned with equipping their own armies with such elements, primarily as a result of the advantages that arise from the options for their use.

From this point towards the direction of hybrid warfare involving the use of such elements was only a step, and this was taken by countries that use this type of unmanned aircraft for military purposes. The big problem, however, became the folding of the advantages of using drones and balloons on the characteristics of hybrid warfare, a situation that has recently exposed a multitude of advantages in terms of the use of such objects, to the detriment of the targeted countries.

HYBRID WARFARE – AT THE CONVERGENCE OF THE MILITARY AND THE NON-MILITARY. WAR BY ALL MEANS

In recent decades, the international security environment has undergone a series of mutations that have complicated developments in the security field through the emergence of a new form of warfare - hybrid warfare. And if previously,

the confrontation between international actors revolved around classic conflicts, specific to past centuries, the emergence of the hybrid dimension of conflicts has come to complicate the situation. In the sense that hybrid wars combine military and non-military means, overt and covert actions, such as disinformation, cyberattacks, economic pressure, the use of regular forces and irregular armed groups, etc., with the aim of blurring the boundaries between war and peace, in order to sow doubt in the minds of target populations, in order to undermine them and implicitly destabilize the respective states (NATO, 2024).

With the emergence of this type of conflict and the awareness of the effectiveness of the magnifying glass taken to the “gray area”, countries that use such actions to achieve their goals have diversified their options for action, so that currently we can explain the tactics of hybrid warfare by bringing into discussion urban guerrilla fighting, disinformation, kidnappings, terrorism, the use of drones and balloons, etc. (Bargués, Bourekba, 2022), in a combination of actions and elements that speak of waging a war by all means at hand, military and non-military.

In other words, hybrid conflict can be explained by the use of a full range of different modes of warfare, which include conventional and unconventional capabilities, involving irregular tactics and formations, acts of terrorism, but also actions that may involve indiscriminate violence and coercion (Hoffman, 2007, p. 8).

Then, also due to the need for a more applied explanation of hybrid warfare, it is useful to divide the elements that can be used in the logic of a hybrid approach to conflict, into military means, that is, the use of what is conventional, including sophisticated weapons, and unconventional, which can mean the covert use of special forces, or the support of groups that can act as proxies. If the military dimension in any conflict remains tributary to that involving equipment and access to technology, the non-military dimension of hybrid offers even more opportunities for actors who resort to this type of confrontation, that is, the use of a wide range of non-kinetic measures. And here we are talking about propaganda and disinformation, as options for spreading fake news and more; cyberattacks and hacking; economic pressure (sanctions, trade restrictions, interruption of the supply of vital resources); diplomatic pressure and related tactics (lawfare); sabotage and terrorism, elements used simultaneously and adaptively in a combined mix to achieve the desired political objectives (Hoffman, Neumeyer, Jensen, 2024).

More recently, the weaponization or instrumentalization of migrants has been added to the list of hybrid threats (Gkliati, 2023), their transformation into a “weapon” demonstrating how any means can be used in this type of confrontation, as long as it can bring advantages to the aggressor.

An important aspect of what it means to wage a hybrid war is that the “dosing” of actions and the “mixing of ingredients” depend on the military strategies of the international actors who resort to such actions, hence the complexity of hybrid wars as a result of the fact that the aggressors use any means at hand to affect the security and stability of the targeted international actors.

The term hybrid warfare is linked to the year 2005 and Lt. Gen. James Mattis of the US Marine Corps, who explained this relatively new type of conflict, and then wrote, together with Lt. Col. Frank Hoffman, a work dedicated to this type of war, called “Future Warfare: The Rise of Hybrid Wars”. Hoffman later continued the effort to popularize this term through a series of essays and books in which he explained hybrid warfare by referring to the 2006 conflict in Lebanon, more specifically to the way in which the Lebanese group Hezbollah acted against the State of Israel, effectively combining high-tech firepower – cruise and anti-ship missiles, with classic guerrilla warfare tactics, to which it added a media campaign directed against the Israeli state.

Identifying the effectiveness of such a combination of actions, Frank Hoffman warned at that time that future adversaries of the United States of America would act relatively similarly, by combining the conventional military dimension with acts of terrorism, cyberwarfare, propaganda, etc., the purpose of this mix of elements being to cause maximum damage to the security of the American state, both physically and psychologically (Baku Network, 2025).

The period that followed partially validated Hoffman’s theory regarding the USA, which is the target of actions that fall within the scope of hybrid warfare, backed by states such as China and the Russian Federation, but the “textbook case” on this dimension is dedicated to Ukraine and the effects that the conflict in Eastern Europe has, especially on countries that are part of the Euro-Atlantic space.

BALLOONS AND DRONES – THE THREAT FROM THE GRAY AREA OF HYBRID WARFARE

The last few decades have witnessed technological developments unprecedented in history, while the emergence of Unmanned Aerial Vehicles (UAVs), also known as drones, has opened up unprecedented opportunities. Unmanned aerial vehicles are aircraft without a crew or passengers on board, and can be automated or remotely piloted, while the ability to fly for long periods of time and over long distances increases their usefulness in both civilian and military use (The Editors of ProCon, 2025).

And the discussion on the military utility of these devices can start from the difference between drones and cruise missiles, two overlapping elements as technology from several points of view, from what it means to use them for guided flights, to almost similar capabilities, while the differences come from the reuse of drones, which are aerial vehicles that return to base after the mission is completed (with the exception of the kamikaze ones), unlike cruise missiles that are destroyed upon reaching the target.

Other differences relate to the fact that a cruise missile generally carries a much larger explosive payload, while drones, due to the technology they are based on, are most often controlled and monitored remotely by the crews that operate them, being programmed to return to base, unlike cruise missiles which, once launched for a mission, operate based on pre-programming, being largely completely autonomous once they have left the launch point (Schmidt, Haider, 2021).

However, discussing the use of drones and balloons in hybrid warfare transcends the military dimension of the conflict, as it is not exclusively about the use of military UAVs in actions against enemies on the battlefield. Rather, it is about incidents involving civilian drones and balloons that paralyze air traffic in the countries where they occur, creating a state of panic in the affected societies, while increasing anxiety among the authorities of the respective states, who are faced with difficulties in how to frame such incidents and how to manage them.

BALLOONS – THE (NEW) FLYING THREATS

Aeronautics explains balloons (Rumerman, n.d.) as unpropelled aerostat objects that, as a result of their characteristics, can remain in the air or float due to their buoyancy, differentiating themselves from vehicles that are part of the airship category, which are propelled aerostat objects that fly in a controlled manner.

The first elements that speak of hot air balloons are related to the history of China, more precisely to the era of the Three Kingdoms, when Zhuge Liang of the Shu Han kingdom (220-280 AD), used aerial lanterns for military signaling (Atkins, 2022).

History also shows that the first inventions used in aerial warfare were balloons and kites, with their main role being reconnaissance, providing an overhead view of the battlefield and the positioning and movements of enemy troops. Later, balloons were used to set fire to enemy targets, while the first recorded military use of balloons is related to the French Revolutionary Wars. The military efficiency of such elements made their use even more widespread starting in the 19th century, and the technological level of those times led to their equipping with cameras, telegraphs

and other instruments that allowed for much more operational, detailed and precise reconnaissance and observation actions, essential in the military dimension (Britannica Editors, 2024).

Nowadays, balloons are not widely used in the military field, with an obvious preference for technologies such as drones and satellites for access to information and monitoring options, but today, centuries after the beginning of the use of this type of aerostat objects, the hybrid war waged by the Russian Federation against countries in the Euro-Atlantic space exposes a complicated reality. The one in which mysterious balloons can have the most diverse effects on the states to which they are sent, including from the perspective of the options these countries have to manage this type of threat coming from the air.

The case of Lithuania and the mysterious balloons that have been flying over its skies since September 2024 is a relevant one in the logic of analyzing the challenges that come in this dimension. In short, during the aforementioned period, dozens of balloons carrying large packages floated from Belarus to Lithuanian airspace. In October 2024, such a balloon landed at Vilnius airport, and it was discovered that the large packages attached to the balloons coming from Belarus contained smuggled cigarettes, and were also equipped with satellite tracking devices to be later recovered by the cigarette smugglers. A few days after the incident involving the balloon landing at Vilnius airport, another similar one landed at a military complex in Lithuania.

At that time, even though evidence indicated that the balloons were only carrying contraband cigarettes, being the only option left for smugglers after Lithuania, in 2023, built a 550 km wall and closed some border crossings on the frontier with Belarus, the Baltic state did not feel comfortable in the context of these developments, especially since the same period coincided with the one in which the Lithuanian authorities made efforts to strengthen defenses on the Eastern border, in an attempt to limit the risks and threats coming from the Russian Federation and Moscow's ally, Belarus. Despite these efforts, in recent times, balloons flying from Belarus have become a common occurrence in Lithuania, with around 250 balloons crossing the border between the two states in September 2024 alone (Seputyte, 2024), a situation that has generated major concerns in the Baltic country.

Then, on 24 November 2024, Lithuania had to deal with the largest flow of balloons entering its airspace to date, so Vilnius Airport had to suspend its operations twice due to balloons in its vicinity, initially for five hours, a period that was later extended. It was not the first disruption of Vilnius Airport's operations, with ten flights and 1,100 passengers affected on 20 November 2024. Earlier,

in October of the same year, as a result of similar incidents, approximately 95 flights were affected and over 14,000 passengers. The decision of the Vilnius regime last autumn to temporarily close the border with Belarus was designed to reduce the number of incidents coming from Belarus and their effects (Kulakova, 2025).

Even if at first glance the balloons can be associated with an action that can be classified as organized crime, more precisely the illicit trafficking of cigarettes, the problem itself is much more complicated. And this complication comes in the context in which it is not excluded that the balloons with trafficked cigarettes test the reaction of the Lithuanian authorities to incidents that are “harmless” at first glance for the security of the Lithuanian state, but much more profound in terms of possible direct and secondary effects in the future, for several reasons. First of all, due to the fact that hybrid warfare is a type of warfare that combines the use of all possible means to create situations that are difficult for the target state to manage. And, starting from this approach in which a hybrid aggressor will transform any offererelement for its stage win into an institutionalized one, the actors behind hybrid actions will use elements related to the unconventional dimension in devising broad strategies that have the ability to circumvent the clear demarcation between what can be considered civilian activity and the security risk for the state in the midst of such a situation.

And from this point of view, it is relevant to analyze the way in which the action is “staged”, and the example of Lithuania is a relevant one, since it is obvious that no balloon carrying smuggled cigarettes left the state border without this being known to the Belarusian intelligence. Hence the more than pertinent assumptions that once the Belarusian KGB accepted such actions, there is no doubt that the actions are known and, most likely, carried out with the acceptance and encouragement coming from Moscow. An assumption that is related to the close relationship between the Minsk regime and the Kremlin, that is, to the fact that from the moment of the start of the so-called “*special military operation*” in Ukraine, the Belarusian state was used by the Russian Federation to prepare and “*cosmeticize*”, at the same time, its bellicose actions against the Ukrainian state (Bajarūnas, 2024).

Given these developments, the question that arises is whether the swarms of balloons carrying contraband cigarettes from Belarus to Lithuania represent an action by smugglers, are they part of Russia’s hybrid war against the Euro-Atlantic space, or are both valid? The Lithuanian Prime-minister has classified the incidents involving weather balloons arriving from Belarus to Lithuania as “*hybrid attacks*”. Analyzing the immediate consequences that the balloons crossing the Lithuanian border generate, interpreting them as related to the intention to create chaos

and “test” the weaknesses of the Lithuanian state is not considered inappropriate. At least not in the context of recent years, marked by the effects of hybrid warfare in the region and the intention of the Russian Federation to create confusion and instability in the states on NATO’s Eastern Flank. Lithuania seems to be at the forefront of this new type of action, while Poland and Latvia have also been affected, in the sense that balloons have also arrived on their territory, but in much smaller numbers.

The signals coming from the Lithuanian authorities regarding the fact that the balloon swarms represent hybrid attacks on the West, being a significant threat to the security of the states on the Eastern Flank, because they are “*committed in the broader context of Russia’s war of aggression against Ukraine*”, raise an alarm regarding the new hybrid challenges. Especially since the biggest fears are that in the near future, such balloons may be equipped with spy cameras, incendiary devices or even explosives, providing Moscow with a tool in mapping the weaknesses of the states on the Eastern Flank (Rothwell, 2025).

Another telling example of the use of balloons and their impact is the incident in 2023 when an alleged Chinese spy balloon flew over North American territories, specifically Canada and the USA, and which American officials believed was a high-altitude surveillance device. This allegation was contradicted by the Beijing regime, which officially reported that the airship was used for meteorological purposes and deviated from the planned route. The situation was, however, a delicate one, given that the Chinese balloon flew over the Aleutian Islands in Alaska, crossed Canada and then arrived in the city of Billings in Montana, a region that hosts several of the US nuclear missile silos (BBC, 2023).

THE USE OF DRONES SEEN THROUGH THE LENS OF HYBRID WARFARE

That military drones have become a defining feature of modern warfare (Clapp, 2025, p. 1) is proven by developments in theaters of operations in Ukraine, the Gaza Strip/Israel, Lebanon, to the civil conflicts in Sudan, Syria and Myanmar, which demonstrate that UAVs have become ubiquitous, as a result of the preference of state and non-state international actors to use this type of military technique in their actions.

Another reality is that drones have changed the tactical dynamics of conflicts, even if there are debates regarding the strategic impact of their use, as argued by those who give examples of the numerous American drone attacks in the Middle East and Afghanistan, and who argue that despite them, the military threat in these

spaces still persists. The same is true in the case of Ukraine (Andersson, Simon, 2024, p. 1), where the large-scale use of drones by both sides has not significantly changed the front lines (Clapp, 2025, p. 2), even if their ability to cause major damage to the enemy is undeniable.

However, discussions about the use of drones in hybrid warfare go beyond the military dimension of their use and reveal a much more complex situation, due to the unpredictability of the situation. Because, in the hybrid war waged by the Russian Federation against NATO and the EU member states, with the exceptions involving the passage of drones used by the Russian Army in attacks in Ukraine into the airspace of countries on the Eastern Flank, recent incidents indicate a situation that is at least complicated.

And to understand this reality, it is more than appropriate to provide an example that has not been sorted as an action that can be classified as hybrid warfare, but which may be relevant to understanding subsequent developments. And here we discuss the incident of December 2018, when hundreds of flights from Gatwick Airport near London were canceled amid reports indicating the presence of drones near the runway. In numbers, the incident translates into around 1,000 affected flights and 140,000 passengers who were impacted by what is considered to be the biggest disruption to Gatwick Airport's activity since the eruption of the Icelandic volcano Eyjafjallajökull in 2010, an eruption that paralyzed air traffic across almost the entire European continent (BBC, 2018).

The period following the incidents near Gatwick Airport was marked by somewhat isolated incidents, but recent years have demonstrated the transformation of events in the same category into a major emergency. An emergency that arises from the increasing number of such events and the need for the authorities of the target states to manage such situations as efficiently as possible, especially since the examples are multiple. Thus, in November 2024, several unauthorized drone flights were reported in the UK over and near the military bases RAF Lakenheath, RAF Mildenhall, RAF Feltwell and RAF Fairford, all considered critical to US military activities in Europe, being considered of strategic importance, as RAF Mildenhall is used for refueling missions and special operations; RAF Feltwell for logistical support provided to US forces; RAF Lakenheath is home to the US Air Force's 48th Fighter Wing; while RAF Lakenheath is scheduled to host US nuclear weapons. Even though British and American officials did not provide details at that time regarding the number of drones involved in the incidents, or who might have been behind them, the events were treated seriously by the two states, which took measures to limit the effects on their security (Peart, 2024; Hearn, 2025).

Germany also experienced similar experiences in August 2024, when it reported suspicious drones near US military bases. Later, in December of the same year, the US confirmed an increase in incidents around military bases in Germany, including the famous Ramstein air base, while some industrial areas, including some owned by the arms manufacturer Rheinmetall, were under observation (Reuters, 2024; France 24, 2024).

Later, the year 2025 proved even more prolific in this regard, with the list of incidents involving unidentified drones being even longer. The first major incident of the year concerned Copenhagen Airport, on September 22 this year, Danish authorities took the decision to suspend activities at this airport for more than four hours, after several drones were observed in its vicinity, classifying the incident as a hybrid operation aimed at disrupting critical infrastructure. On the same night, Norwegian authorities made the same decision, temporarily suspending the activity of Oslo Gardermoen Airport for similar reasons.

Between September 24 and 26, similar incidents occurred near Aalborg Airport in Denmark, which has a dual purpose, civil and military, as it also hosts a military base, the activity of this airport being disrupted in two different situations, while the airports of Esbjerg, Sønderborg and Flyvestation Skrydstrup were also affected, with the latter being the main air base of the Royal Danish Air Force, which hosts the 30 F-16 Fighting Falcon fighter jets in the Danish Air Force's fleet (Jacobsen, 2025). The incidents that affected Denmark came in the context in which this state holds the rotating presidency of the Council of the European Union (July – December 2025), but also a few days before a meeting of the EU Council that took place in Copenhagen, on October 1 this year. The topics of discussion on the agenda of the leaders of the EU states included measures to strengthen the common defense of Europe, with a focus on the violations of airspace by the Russian Federation in several European states (European Council, 2025), a topic that has become increasingly urgent and topical in the context of the challenges of hybrid warfare.

The above incidents are not unique, as Poland has also been the target of similar actions. Specifically, on the evening of September 9, between 19 and 23 unarmed drones entered Polish airspace. Polish Prime-minister Donald Tusk described this type of action, which involved the entry of foreign drones into Polish airspace, as a *"direct threat"*. Poland went even further and invoked Article 4 of the North Atlantic Treaty (Hubenko, Ford, Connor, Hairsine, 2025), an article that provides for the possibility for NATO member states to request consultations with other members of the organization in the event that they consider that the territorial integrity, security and political independence of the respective state are threatened (NATO, 2025).

Poland's justification for such a decision to request consultations was explained by Deputy Prime-minister Radosław Sikorski, who brought up the fact that the incidents that affected Poland, including the disruption of the activities of the airports: Warsaw International Airport, Warsaw Modlin Airport, Rzeszów – Jasionka Airport and Lublin Airport, which were temporarily closed, represent *“an unprecedented case of attack not only on the territory of Poland, but also on the territory of NATO and the EU”* (Polskie Radio PL, 2025).

In the context of recent developments, the concerns of the two international organizations and the states on the front lines of hybrid warfare are more than evident.

Amid a growing number of events involving foreign drones, NATO announced on 27 September 2025 that it would increase its presence in the Baltic Sea by boosting intelligence activity and deploying the frigate FGS Hamburg, in a reinforcement of the NATO *“Baltic Sentry”* mission that began in January this year in response to a series of incidents involving damage to electrical cables, telecommunications links and gas pipelines on the Baltic Sea floor. Another NATO mission, *“Eastern Sentry”*, was launched in September this year to increase the defense of the Alliance's Eastern Flank, in response to threats generated by Russian drones violating Polish airspace (Sytas, 2025).

At the EU, the head of the European Commission, Ursula von der Leyen, sounded the alarm that *“something new and dangerous is happening in our skies”*, a statement made on 8 October 2025, in front of the European Parliament. The head of the European Commission signaled the need for a reaction from the EU, explaining that *“one incident can be a mistake. Two, a coincidence. But three, five, ten? This is a deliberate and targeted campaign in the grey area against Europe. And Europe must respond.”* (Lecca, 2025).

INSTEAD OF CONCLUSIONS

Awareness of the challenges that international state and non-state actors in the Euro-Atlantic space face in the hybrid dimension is a mandatory condition for taking pertinent and coherent measures in the fight against an invisible enemy. In the sense that, despite the attribution, in the vast majority of cases in Europe, of responsibility for incidents in this space to the Russian Federation, the use of drones and balloons represents an option that can be included in hybrid warfare that comes with a series of advantages for the hybrid aggressor, advantages that are directly proportional to the threats that these actions pose for the target state.

And on this dimension, the characteristics of the hybrid dimension involving the use of drones and balloons are of reference, starting from the fact that they represent cheap elements, which can be used without involving high material costs. Moreover, the fact that in few cases the incidents involving drones and balloons could be attributed to the states that initiated them, in the sense of holding them accountable, reduces to almost a minimum the political costs for hybrid aggressors, which benefit from the strategic consequences that the use of such elements implies, that is, the option to create chaos and affect the security of the target states, without resorting to the military component.

Or from this point of view, the fact that the use of drones and balloons can create anxiety in the capitals of the targeted states, while the level of discomfort felt by their societies is high, we could say that such actions that can be classified as hybrid warfare generously expose more than attractive options and opportunities for the actor using them.

BIBLIOGRAPHY:

1. Andersson, J.J., Simon, S. (2024). *Drone warfare and the EU*. European Union Institute for Security Studies, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_2024-17_Drones%20%281%29.pdf, retrieved on 24 November 2025.
2. Atkins, H. (2022). *When Were Hot Air Balloons Invented?* HistoryHit, <https://www.historyhit.com/when-were-hot-air-balloons-invented/>, retrieved on 12 November 2025.
3. Bajarūnas, E. (2024). *Beware – Mystery Balloons Can Carry a Punch*. CEPA, <https://cepa.org/article/beware-mystery-balloons-can-carry-a-punch/>, retrieved on 24 November 2025.
4. Baku Network (2025). *Hybrid Warfare: The Invisible War That's Already*, <https://www.bakunetwork.org/en/news/analytics/14514>, retrieved on 27 September 2025.
5. Bargués, P., Bourekba, M. (2022). *War by all means: the rise of hybrid warfare*. Barcelona Center for International Affairs, <https://www.cidob.org/en/publications/war-all-means-rise-hybrid-warfare>, retrieved on 12 September 2025.
6. BBC (2018). *Gatwick Airport: Drones ground flights*, <https://www.bbc.com/news/uk-england-sussex-46623754>, retrieved on 24 November 2025.
7. BBC (2023). *Chinese spy balloon over US is weather device says Beijing*, <https://www.bbc.com/news/world-us-canada-64515033>, retrieved on 24 November 2025.
8. Britannica Editors (2024). *"Balloon"*. Encyclopedia Britannica, <https://www.britannica.com/technology/balloon>, retrieved on 12 November 2025.
9. Clapp, S. (2025). *Military drone systems in the EU and global context: Types, capabilities and regulatory frameworks*. European Parliamentary Research Service, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/772885/EPRS_BRI\(2025\)772885_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/772885/EPRS_BRI(2025)772885_EN.pdf), retrieved on 24 November 2025.
10. European Council (2025). *Informal Meeting of the EU Heads of State or Government*, Copenhagen, 1 October 2025, <https://www.consilium.europa.eu/ro/meetings/european-council/2025/10/01/>, retrieved on 24 November 2025.

11. France 24 (2024). *Unidentified drones seen over US military base, industrial site in Germany*, <https://www.france24.com/en/europe/20241213-unidentified-drones-seen-over-us-military-base-industrial-site-in-germany>, retrieved on 24 November 2025.
12. Gkliati, M. (2023). *Let's Call It What It Is: Hybrid Threats and Instrumentalisation as the Evolution of Securitisation in Migration Management*. *European Papers – A Journal on Law and Integration*, <https://www.europeanpapers.eu/europeanforum/lets-call-it-what-it-is-hybrid-threats-and-instrumentalisation>, retrieved on 17 September 2025.
13. Hearn, J. (2025). *Nearly 200 drone sightings near UK military bases since the start of the year, MOD confirms*. RAF, <https://www.forcesnews.com/services/raf/nearly-200-drone-sightings-near-uk-military-bases-start-year-mod-confirms>, retrieved on 24 November 2025.
14. Hoffman, F.G. (2007). *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington: Potomac Institute for Policy Studies, retrieved on 20 November 2025.
15. Hoffman, F., Neumeyer, M., Jensen, B. (2024). *The Future of Hybrid Warfare*. Center for Strategic&International Studies, <https://www.csis.org/analysis/future-hybrid-warfare>, retrieved on 17 September 2025.
16. Hubenko, D., Ford, M., Connor, R., Hairsine, K. (2025). *Poland calls NATO meeting after downing Russian drones*, DW, <https://www.dw.com/en/poland-calls-nato-meeting-after-downing-russian-drones/live-73941525>, retrieved on 24 November 2025.
17. Jacobsen, S. (2025). *Denmark links drones at Copenhagen airport to hybrid attacks across Europe*. Reuters, <https://www.reuters.com/world/europe/drones-that-shut-copenhagen-airport-flown-by-capable-operator-danish-police-say-2025-09-23/>, retrieved on 24 November 2025.
18. Kulakova, M. (2025). *Lithuania Reports "Most Intense" Belarus Balloon Launches in November, Latvia Hit Too*. United24Media, <https://united24media.com/latest-news/lithuania-reports-most-intense-belarus-balloon-launches-in-november-latvia-hit-too-13719>, retrieved on 24 November 2025).
19. Lecca, T. (2025). *'Hybrid warfare' or more of the same? Getting a grip on drones across Europe*. Politico, <https://www.politico.eu/article/hybrid-warfare-or-more-of-the-same-getting-a-grip-on-drones-across-europe/>, retrieved on 24 November 2025.
20. NATO (2024). *Countering hybrid threats*, <https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats>, retrieved on 12 September 2025.
21. NATO (2025). *The consultation process and Article 4*, <https://www.nato.int/en/what-we-do/introduction-to-nato/the-consultation-process-and-article-4>, retrieved on 24 November 2025.
22. Peart, H. (2024). *Drones spotted over military bases in the U.K. that are used by the U.S.* NBS News, <https://www.nbcnews.com/news/world/drones-seen-near-us-bases-uk-air-force-rcna181971>, retrieved on 24 November 2025.
23. Polskie Radio PL (2025). *Poland summons Russian envoy over drone incursions: FM*, <https://www.polskieradio.pl/395/7784/artykul/3577733,poland-summons-russian-envoy-over-drone-incursions-fm>, retrieved on 24 November 2025.

24. Reuters (2024). *Alert at NATO base in Germany was due to drone threat, source says*, <https://www.reuters.com/world/europe/alert-nato-base-germany-was-due-drone-threat-source-says-2024-08-26/>, retrieved on 24 November 2025.
25. Rothwell, J. (2025). *Russia's new weapon in hybrid war against Europe*. The Telegraph, <https://www.telegraph.co.uk/world-news/2025/11/28/russia-new-weapon-hybrid-war-against-europe/>, retrieved on 28 November 2025.
26. Rumerman, J. (n.d.). *Early Balloon Flight in Europe*. U.S. Centennial of Flight Commision, https://web.archive.org/web/20080701154629/http://www.centennialofflight.gov/essay/Lighter_than_air/Early_Balloon_Flight_in_Europe/LTA1.htm, retrieved on 12 November 2025.
27. Schmidt, A., Haider, A. (2021). *The Differences between Unmanned Aircraft, Drones, Cruise Missiles and Hypersonic Vehicles*. Joint Air Power Competence Centre, <https://www.japcc.org/chapters/c-uas-the-differences-between-unmanned-aircraft-drones-cruise-missiles-and-hypersonic-vehicles/#cruise-missiles-versus-unmanned-aircraft>, retrieved on 18 September 2025.
28. Seputyte, M. (2024). *Mystery Hot-Air Balloons Unnerve a Jittery Lithuania*. Bloomberg, <https://www.bloomberg.com/news/newsletters/2024-10-05/mystery-hot-air-balloons-unnerve-a-jittery-lithuania>, retrieved on 10 October 2025.
29. Sytas, A. (2025). *NATO to increase presence in the Baltic after Denmark drone incidents*. Reuters, <https://www.reuters.com/world/nato-step-up-vigilance-baltic-after-denmark-drone-incidents-2025-09-27/>, retrieved on 24 November 2025.
30. The Editors of ProCon. (2025). *"Drones"*. Encyclopedia Britannica, <https://www.britannica.com/procon/drones-debate>, retrieved on 12 November 2025.

RESILIENCE OF INTELLIGENCE SERVICES IN THE ERA OF HYBRID WARFARE

Dr. Răzvan CURCULESCU

Resilience Core Initiative Association-Thor member, Bucharest

DOI: 10.55535/RMT.2025.3.24

This article provides an exhaustive examination of the operational and institutional resilience of intelligence services in NATO and EU countries in the context of the hybrid war waged by the Russian Federation, as well as the clarification and delimitation of the concept of resilience, as reflected in the programmatic documents of organizations relevant in the field of security, analyzing the measures that can contribute to increasing the resilience of intelligence services, by correlating them to the effects of hybrid warfare on all dimensions of democratic society.

In a period deeply marked by the growth of disinformation, the diversification of cyber-attacks and the increase in the dynamics of influence actions led by state actors, a doctrinal and institutional reset is necessary, as well as the consolidation of cooperation at the level of partner services, through a comparative analysis of public, security policies and strategic documents, highlighting the conceptual and operational differences of NATO and EU states, but also the elements of convergence in the field of resilience from the perspective of designing an integrated intelligence architecture.

Keywords: hybrid warfare; resilience; intelligence services; NATO; EU;

CONCEPTUAL APPROACHES – FROM HYBRID WARFARE TO RESILIENCE

The concept of *hybrid warfare*, enunciated and analyzed by Hoffman in 2007, designated an activity aimed at identifying and exploiting the systemic vulnerabilities of a state considered a target, through actions and operations that do not represent a direct confrontation. In the current period, we observe that hybrid warfare has become part of the strategic confrontation between powers, manifesting itself through the combination of conventional and unconventional means (Hoffman, 2007, p. 8), such as cyber, informational, energy, economic and more.

If hybrid warfare was initially linked to the 2006 Lebanon conflict, in the last decade it has been observed that the **Russian Federation** combines conventional and unconventional means, military and non-military, in a coordinated campaign aimed at achieving political and military objectives, in a first stage, without declaring an open war. Through instruments such as: cyber operations, disinformation campaigns, economic or energy pressures, the use of proxy actors (militia, mercenaries, criminal organizations), political and psychological interventions, sabotage, drone incursions, its aim is to divide and weaken the adversary's decision-making capacity, without a classic confrontation (Mumford, 2020, pp. 3-4; Galeotti, 2016, pp. 5-9).

Hybrid warfare exploits the modern "*fog of war*" (Mumford, 2020, p. 5). Hybrid actors, state or non-state, simultaneously launch massive flows of contradictory information (fake news, fabricated sources, manipulated data), designed to saturate the analytical capacity of the adversary, and the examples below, which present real examples that can be classified as this type of war, highlight the difficulty of countering such actions.

- a. **Erosion of information certainty** – in the hybrid war waged/carried out by the Russian Federation, truth has become a battlefield. The Russians use **disinformation, deepfakes, source manipulation and controlled leaks** to pollute the information environment. The aim is twofold: to **divert the internal analysis** of the intelligence structures of the targeted countries and to **undermine the trust of decision-makers** in their own information apparatus. Thus, during the conflict in Ukraine (2022-2024), Russia simultaneously launched contradictory narratives ("*there is no invasion*")/

“liberation operation”), generating confusion including in OSINT flows. Western services countered Russian attacks on this dimension **through multi-domain fusion and collaborative analysis NATO-EU-Ukraine** (NATO StratCom COE, 2023).

- b. **Increasing pressure on cyber infrastructure (technological resilience)** – hybrid warfare includes attacks on the **IT infrastructure of intelligence services** – classified servers, encrypted channels, operational databases or SCADA systems. These attacks are intended to **temporarily “blind” the capacity for analysis and response**. In 2021, attacks on government networks in Ukraine and Poland (the *“Ghostwriter”* and *“Sandworm”* campaigns) demonstrated how an adversary can temporarily paralyze strategic intelligence communication. NATO and the EU have provided joint support through the CCDCOE and Hybrid CoE, testing crisis response (ENISA, 2022).
- c. **Human and organizational overstrain (organizational resilience) – hybrid warfare implies continuous activity, permanent uncertainty and media pressure**. Intelligence services, accustomed to linear information cycles, must now operate in a constant alert mode. After 2014, the Baltic services (Estonia, Latvia, Lithuania) introduced continuous training programs in psychological resilience for intelligence analysts, precisely to counteract the effects of Russian information warfare (Hybrid CoE, 2021).
- d. **Threat to public credibility (societal resilience)** – hybrid adversaries not only attack information networks, but also **the public image of intelligence institutions**, with the aim of losing public trust and isolating the services from their own government. In disinformation campaigns in Central Europe (2018-2022), the services were direct targets: false accusations of domestic espionage or corruption aimed at weakening public trust. The Nordic countries countered through strategic communication resilience programs coordinated with NATO StratCom COE (Riga).
- e. **Changing the defense paradigm (systemic resilience)** – hybrid warfare forces the transition from the classic paradigm – *“intelligence reacts to threats”* – to a proactive and integrated one: *“intelligence prevents and shapes the security environment”*. The NATO JISR (Joint Intelligence, Surveillance and Reconnaissance) model and the EU-SIAC partnership are concrete examples of **integrated systemic resilience**, which ensures information continuity even in the event of the degradation of an intelligence node (NATO, 2020; EEAS, 2022).

Based on the examples above, it is clear that hybrid warfare forces intelligence services to become **living and adaptive organisms**, capable of operating in ambiguity and continuous pressure. Their resilience no longer depends solely on technology or secrets, but on the **balance between people, information and trust**. In the hybrid era, the strongest intelligence service is not the one that knows the most, but the one that **resists uncertainty the best** (Hybrid CoE, 2023, pp. 4-6; Linkov, Kott, 2019, pp. 3-5).

Thus, we can say that hybrid warfare acts as a **permanent stress test** for intelligence services, forcing them to rethink their mission, structure and internal culture, while resilience no longer means just survival after an attack, but also the **ability to function effectively in continuous uncertainty**.

Against the backdrop of hybrid warfare, intelligence services have become the main institutions that contribute to strengthening the resilience of target states, pillars of strategic resilience, by carrying out early warning and decision-making protection missions.

Conceptually, we will define resilience as the capacity of a system to absorb shocks and maintain its essential functions in crisis situations. Adapting the concept to the subject of this research, we can consider that the resilience of intelligence services represents the state in which they are operationally, organizationally and cognitively adapted to deal with crisis situations generated by hybrid warfare.

In the specialized literature we find the concept of resilience treated from different perspectives – *societal resilience* (Chandler, 2014, p. 56), *technological resilience* (Linkov, Trump, 2019, pp. 9-34), but that of *state resilience*, strategic or punctual resilience, of intelligence services, is a field in which this concept is relatively new. An important point in its definition is the moment of the illegal annexation of the Crimean Peninsula by the Russian Federation (2014), which led NATO and the EU to conceptualize the notion of resilience at the level of the two international organizations.

In 2022, NATO (NATO, 2022) and, subsequently, the EU in 2023 (ENISA, 2023), launched a series of policies aimed at strengthening the resilience of states against the threats of hybrid warfare, highlighting cyber threats and information aggression as high-risk factors affecting the security of member states. In that context, we can see the establishment of the principle that the resilience of intelligence services was directly influenced by the adaptation of operational capabilities to this new type of threats. We withhold here the reference framework established by NATO by defining the “seven basic requirements for resilience” (NATO, 2016, para. 73),

but also the mechanisms established by the EU through the Hybrid Fusion Cell (European Commission & High Representative, 2016, Hybrid Fusion Cell section) and the Cybersecurity Strategy (European Commission, 2020).

The comparative analysis of how the two organizations approach the concept of resilience will highlight elements of divergence and convergence, but will emphasize that the resilience of Western intelligence services will not be achievable in the absence of deep cooperation.

The study of data from the public space reveals that the term resilience has a complex meaning. Starting from the theoretical approach that shows that a system, whatever it may be, is resilient if it has the capacity to maintain its basic functions in the event of crises, we observe that in the case of intelligence services these crises, which we can also call disruptions, can be related to terrorism, espionage, cyber-attacks, energy and even economic crises.

We note that in the field of security and, especially in the area of intelligence, the concept of resilience will include as main actors the states, with all their component elements that need to be defended, regardless of the type of threats generated by hybrid warfare. In other words, the resilience of intelligence services becomes a guarantor of the ability of states to manage threats and recover their basic functionalities in the event of security incidents. In this way, states will succeed in maintaining social and political stability, necessary for economic development and maintaining the rule of law.

Against this background, the resilience of intelligence services will be given by their ability to anticipate threats and to adapt proportionate measures in order to protect democratic values, critical infrastructures and public policies. Anticipation is one of the most difficult and complex missions in the intelligence area (Lowenthal, 2017, p. 148) and cannot be achieved in the absence of an increase in the capacity to obtain information, including through cooperation, but especially by increasing their strategic analysis capacity. Experience has shown that the adaptation of intelligence services is given, first of all, by the ability of these structures to learn quickly and efficiently from their own activity but also from the experience of partners.

Therefore, starting from the general interpretation of resilience, we can consider that the resilience of an intelligence service represents the ability to anticipate, manage, counteract and recover from a crisis (disruption). To support the argument, disruption will be understood as any direct or indirect action that was not anticipated, such as: information leaks, cyber-attacks, political pressures, information manipulation or major dysfunction (economic, political, social, military).

Based on these conceptual approaches, in the context of threats specific to hybrid warfare, the characteristic elements of the resilience of intelligence services in the Euro-Atlantic space can be detailed, by grouping them by dimensions, as follows:

❖ **Organizational** resilience (Lengnick-Hall, Beck, Lengnick-Hall, 2011, p. 244), as the manner in which intelligence services manage, through the practice of modern management and an organizational culture based on leadership, to quickly adapt the organization to operational changes that may cause disruptions in the specific activity. Optimal organizational adaptation to technological and geopolitical changes generated by hybrid warfare will be a key factor in maintaining the trust and morale of those who work in this field, in order to fulfill the missions of the services of which they are part.

❖ **Informational** resilience (Wardle, Derakhshan, 2017, p. 16) – is represented by the increase in the quality of information obtained and the superior capacity for analysis and integration of these in order to be able to recognize and counter attacks against intelligence services. In general, attacks can be of the type of fake news or disinformation regarding the role and place of a service in a democratic state. Although very rare in the Euro-Atlantic space, there have been situations in which certain individuals have betrayed the interests of some services and, implicitly, of the states of origin. Against this background, informational resilience will be achieved in the situation in which intelligence services will adapt internal rules in such a way as to prevent possible infiltrations, leaks of information, double sources or even betrayals.

If the two dimensions are very much related to the intrinsic capacity of intelligence services to be resilient and most of the time the listed aspects are less known to the general public, the following dimensions of intelligence services' resilience are usually visible and likely to seriously affect the security of the states they are part of and implicitly the security of the Euro-Atlantic space.

❖ **Operational** resilience (Duchek, 2020, p. 215) of intelligence services is given by the permanent capacity to obtain, analyze and exploit strategic information even when there are crisis situations. Hybrid warfare will constantly generate new, sometimes unforeseen, situations by capitalizing on new innovative technologies, while exploiting vulnerabilities. We are considering here a possible cyber-attack or an act of sabotage on critical infrastructures.

❖ **Societal** resilience refers to the capacity of a society to absorb major shocks (natural disasters, pandemics, economic crises, etc.), to adapt and recover from the shock (Chandler, 2014, p. 56), so we will consider that, in a democratic state,

an intelligence service will have an important place in the societal dimension, as an integral part of society, with a well-defined role of defending the population, strategic decisions, and critical infrastructures against the new challenges generated by hybrid warfare.

❖ **Strategic** resilience (Hamel, Välikangas, 2003, p. 52) is, in the author's opinion, the most important dimension of an intelligence service in the event of major disruptive factors such as those specific to hybrid warfare. The role of an intelligence service in maintaining the decision-making capacity of a state in times of major crisis (war or severe damage to critical infrastructure) is essential in a democratic state.

THE RESILIENCE OF INTELLIGENCE SERVICES IN EURO-ATLANTIC STRUCTURES

To better understand the field, we will conduct a comparative analysis of how resilience is approached at NATO and EU levels, while also presenting a series of considerations regarding how Romania approaches this field.

The North Atlantic Treaty Organization/NATO is a political-military alliance formed in 1949 with the primary purpose of ensuring the collective defense of its member states. NATO is *"a political and military alliance of countries in Europe and North America, the purpose of which is to guarantee the freedom and security of its members by political and military means"* (NATO, What is NATO?).

The European Union/EU is a political and economic union of 27 European states that have decided to cooperate closely to ensure peace, stability and prosperity on the continent. The EU's main role is to facilitate cooperation between member states so that they are stronger together than apart, maintaining peace and supporting economic and social development (EU, What is the European Union?).

Given the very definitions of the two organizations, it can be deduced that resilience is also approached on the specifics of each organization, but the policies and strategies adopted converge towards the same objective, namely, increasing resilience. Both organizations, NATO and the EU, have developed a mix of policies and strategies through which the resilience of intelligence services is built, but also common structures dedicated to integrated analysis, the conduct of joint exercises and the improvement of the legislative framework necessary to strengthen cooperation. Thus, we can say that an effect of the threats of hybrid warfare is also the strengthening of political-military cooperation with civil society to increase societal resilience, especially to cyber-attacks and disinformation.

RESILIENCE OF INTELLIGENCE SERVICES IN NATO

From studying the organization's planning and leadership documents (NATO, Resilience Committee, 2022), it is found that NATO considers **resilience to be the key element** in its policy of deterring hybrid warfare threats, by permanently requesting allies to permanently take the necessary measures to ensure operational capabilities in crisis situations. According to NATO, *"national and collective resilience capacity is an essential basis for the credibility of deterrence"* (NATO, 2024).

NATO initiated, supported and developed the concept of joint deterrence capabilities and supported the establishment of **integrated analysis structures**, such as the Joint Intelligence and Security Division (JISR) and the NATO Intelligence Fusion Centre (NIFC) (NATO, 2024). In particular, the work of these structures has increased the exchange of information between Allies and, consequently, has contributed to increasing the quality of operational decisions. For example, the NIFC *"provides SACEUR (Supreme Allied Commander Europe) with relevant, accurate and timely information to support the planning and execution of operations"* (NATO Intelligence Fusion Centre, "Mission" section).

In the field of cyber defense, NATO has launched a series of **joint exercises** through which partner states can train their specialists by participating in such formats. For example, through the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) in Tallinn, NATO creates realistic defense scenarios that increase the resilience of intelligence services in the context in which they have become increasingly dependent on digital infrastructures. Through these joint exercises, intelligence services have developed the capacity for interoperability and adequate response to threats specific to hybrid warfare.

In essence, NATO's defense doctrine considers military resilience to include the civil and commercial readiness that the military force needs to deploy troops rapidly and freely throughout the Alliance (NATO, 2022, section on *"layered resilience"*). A final aspect that we consider in analyzing the increase in intelligence resilience is the fact that NATO has pursued and succeeded in **unitary standardization of communication** at the Alliance level.

Through instruments such as **Joint Intelligence, Surveillance and Reconnaissance (JISR)** – *an integrated framework in the military field that combines intelligence, surveillance and reconnaissance capabilities to support strategic and operational decisions* and **Federated Mission Networking (FMN)** – which is a NATO initiative aimed at the rapid and interoperable creation of mission networks for allied and partner forces in joint operations, NATO has reduced the risk of *"single points of failure"* in joint operations.

As a conclusion of how resilience contributes to collective defense, we mention the Allied Joint Doctrine in the Allied Joint Publication (AJP) which emphasizes that *“the formation of combined power ... requires layered resilience in the context of defense.”* (NATO, 2022, p. 73).

RESILIENCE OF EU MEMBER STATES' INTELLIGENCE SERVICES

In the context of the intensification of hybrid threats generated by the actions of the Russian Federation, especially cyber, but also of a security environment with a rapid dynamic of evolution and, implicitly, a change in the strategic environment, the EU has adopted a series of political and normative instruments with the aim of strengthening its strategic resilience with a direct impact on strengthening the resilience of intelligence services.

To provide greater clarity on this topic, in this article we will review the key elements of EU measures that contribute to the strategic and operational resilience of intelligence services in EU Member States, such as: Strategic Compass and Single Intelligence Analysis Capacity (SIAC); tools against hybrid threats; cyber regulations and standards; practical cooperation and joint capabilities.

- a. **Strategic Compass & SIAC (Single Intelligence Analysis Capacity).** The Strategic Compass is the EU's strategic guidance document in the field of security and defence, adopted by the Council of the European Union in March 2022, which sets out concrete objectives by 2030 to strengthen resilience, through measures to increase European capacities for anticipation, risk assessment and crisis management. The Strategic Compass is built on four pillars (*“Act”, “Invest”, “Partner” and “Secure”*) and includes measures to anticipate, deter and respond to threats. (Council of the EU, 2022).

In this context, SIAC, which includes EU INTCEN (the civilian intelligence component) and EUMS-INT (the military component within the EU General Staff), was designed as a single point for integrated strategic analysis, with a central role in providing knowledge (Blockmans, Crosson, Paikin, 2022 pp. 4-6).

Its structuring as a *“single entry point”* for strategic analysis provided by member states has allowed the integration of civil and military intelligence flows with the aim of increasing the quality of common analytical products. The introduction of this mechanism has resulted in increased coherence of strategic decisions at the level of EU decision-makers and a clearer overview of hybrid warfare threats. Against this background, the EU has strengthened its strategic resilience for managing complex crises.

b. Cyber regulations and standards. NIS2 and the role of ENISA – the new NIS2 (Network and Information Security Directive) is the EU’s fundamental legal framework for ensuring a high common level of cybersecurity in essential sectors. It represents the most comprehensive European legislative framework for protecting critical infrastructures and extends security requirements to several sectors — energy, transport, health, public administration, telecommunications, finance, digital service providers, etc. (EU, Directive 2022/2555).

The main effects of NIS2 on resilience include: clear obligations to prevent, detect and promptly report cyber incidents; governance and risk management requirements at the level of the management of organizations; minimum standards for network and supply chain security; more severe sanctions for non-compliance. Thus, this Directive introduced strict elements regarding risk management, incident reporting and cross-border cooperation.

The European Union Agency for Cybersecurity (ENISA) plays a central role in the knowledge and implementation of cyber directives. With an extensive role in the implementation of binding EU legislation, ENISA provides: technical guidance and best practices, coordination of responses between Member States, threat assessments (Threat Landscape Reports), support for testing and auditing of critical infrastructures.(EU, 2019, art. 8–11).

Together, NIS2 and ENISA raise the overall level of **cyber hygiene** reduce structural vulnerabilities and narrow the attack surface exploitable by adversaries – essential for the resilience of intelligence services, their digital infrastructures, critical infrastructures and, ultimately, of Member States (EU-ENISA, 2023, pp. 6-7).

c. Tools against hybrid threats. In cooperation with NATO, the EU has created the *European Centre of Excellence for Countering Hybrid Threats* (Hybrid CoE), which is the main platform for cooperation in the joint management of hybrid threats (European Commission& High Representative, 2016, *Hybrid Threats Section*).The Centre functions as a hub of expertise for the identification, analysis and responses to hybrid threats, in areas such as: disinformation and manipulation campaigns, foreign political interference, information warfare, economic and energy pressures, the combination of cyber operations and physical actions (sabotage, border provocations, etc.).

Hybrid CoE not only produces complex analyses and scenarios, but also organizes multilateral exercises, applied training and joint projects. In this way,

the center strengthens societal resilience and sectoral response capacity, in the following directions:

- increases the capacity of institutions to recognize and counter interference;
- provides tools for a coordinated response between sectors (government, infrastructure, private sector);
- contributes to the synchronization of measures between the EU, NATO and participating states.

d. Practical cooperation and joint capabilities. In addition to institutional and normative frameworks, the EU has also invested in operational tools that contribute to interoperability between intelligence services. These tools play a major role in increasing the resilience of these services in managing the Russian Federation's hybrid threats. In this dimension, the following elements are relevant:

- **Space and satellite capabilities** (e.g. Galileo, Copernicus), which provide secure communications, advanced imaging and monitoring of critical environments.
- **Geospatial imaging and analysis centres**, which support the **Common Security and Defence Policy** (CSDP) and crisis response.
- **Permanent Structured Cooperation** (PESCO) initiative, aimed at creating joint capabilities (e.g. medical commands for maritime surveillance, secure communication networks).
- **CSDP projects** including joint training, information sharing and the development of crisis management tools.

In conclusion, through the above, the EU has managed to design an architecture aimed at strengthening the resilience of states and implicitly of intelligence services, these mechanisms being likely to strengthen the resilience of the EU as a whole by creating an integrated security environment, capable of generating adequate reactions to the continuously evolving threats generated by the Russian Federation.

ROMANIA'S OPTIONS AS A NATO AND THE EU MEMBER

Since 2014, in the context of the illegal annexation of the Crimean Peninsula, Romania has initiated a broad process of **doctrinal alignment** with NATO and EU standards, reflected in the *National Defense Strategy (2020-2024)* and in internal reforms of the intelligence services. Based on these, **national resilience** can be understood as the **capacity of state institutions, the economy and society to protect essential functions, to prevent and manage major disruptions and**

to quickly return to a state of normality, in line with the “*extended national security*” approach defined in the National Defense Strategy (Presidential Administration, 2020, pp. 7-8).

In addition to these guidelines, the key institutions involved in the implementation of security, intelligence and resilience policies in Romania are also indicated:

❖ **The Romanian Intelligence Service (SRI)** is the main domestic intelligence service of Romania and acts as the *national authority* in the field of cybersecurity. In this role, the SRI coordinates **cyber resilience** policies, manages the protection of critical infrastructures of national interest and ensures the prevention, detection and counteraction of cyber and terrorist threats. Through the National Cyberint Center and through cooperation with the National Directorate of Cyber Security/DNSC, the SRI contributes to strengthening national incident response capabilities and counters complex cyber-attacks (Ib., pp. 26-27, 34).

❖ **The Foreign Intelligence Service (SIE)** is responsible for collecting, analyzing and providing decision-makers with information on **external risks and threats** to Romania. In the context of national resilience, SIE monitors geopolitical developments, international crises, hybrid risks, cyberattacks originating from outside the country, as well as hostile actors. SIE also coordinates international cooperation with partner services, organizations such as NATO and the EU, and facilitates the exchange of strategic information relevant to national security, the service being responsible for assessing external risks and international cooperation. Against the backdrop of hybrid warfare, the SIE has intensified cooperation with EU structures, participating in the analytical flows of **INTCEN** and the **Hybrid Fusion Cell** (Foreign Intelligence Service, n.d., Mission and international cooperation).

❖ **The Supreme Council of National Defense (CSAT)** represents the **strategic level of integration** of security, defense and intelligence policies. The Council approves national strategies (e.g.: National Defense Strategy, Cyber Security Strategy, etc.), establishes priorities in the information-operational field, coordinates the activity of intelligence institutions and validates the necessary measures to strengthen national resilience. CSAT functions as a unified decision-making platform between the President of Romania, the Government and the structures with responsibilities in the field, functioning as a strategic integrator of intelligence and resilience policies.

Romania began to develop, after 2020, a **cognitive resilience component**, focused on strategic education and combating disinformation. Campaigns such as #SiguranțaOnline (DNSC, 2022) and university programs in *cyber diplomacy*

and *strategic analysis* contribute to the formation of a “*culture of resilience*” in the public space.

In cooperation with StratCom COE, Romania implemented strategic communication exercises and information crisis management simulations, including disinformation scenarios during elections. This societal dimension complements the technological resilience architecture, bringing to the forefront the idea of **cognitive security** – defending the collective ability to distinguish truth from manipulation (Waltzman, 2017, p. 2).

Although Romania has made significant progress, in the author’s opinion, a number of structural vulnerabilities persist: institutional fragmentation between SRI, SIE and other government agencies; shortage of personnel specialized in data analysis and digital intelligence; technological dependence on external providers in the government IT infrastructure; still rigid legislation on data exchange between institutions. However, these challenges are partially offset by international cooperation and the continuous process of institutional learning.

The comparative analysis of the way Romania approaches the concept of resilience in relation to NATO and the EU, highlighted the fact that our country is positioned in an area of **doctrinal convergence** between the two Euro-Atlantic organizations. This strategic positioning is not only a consequence of dual membership, but the result of a **deliberate policy of institutional adaptation**. In the author’s opinion, in the last ten years, the intelligence services in Romania have moved from a defensive paradigm, focused on information protection, to a proactive one, based on **anticipation, sharing and adaptability**.

Through constant cooperation with **NATO centers of excellence (CCDCOE, StratCom COE)** and participation in European analysis mechanisms (INTCEN, Hybrid Fusion Cell), Romania has developed a multiple resilience, combining military, civilian and cognitive capabilities, so that Romania is described in the specialized literature as an “*emerging cybersecurity hub*” in Eastern Europe (Popescu, 2022). However, this positioning also brings vulnerabilities, especially since the geographical proximity to conflict areas (Black Sea, Ukraine, Republic of Moldova) amplifies the pressure on the intelligence structures in our country.

In the field of intelligence, **cognitive resilience** refers to the ability of analysts and decision-makers to recognize, interpret and react to manipulative information. This is closely linked to **institutional resilience**, which involves flexible structures and rapid information flows. Out of the need to deal as effectively as possible

with the current challenges it faces, Romania has begun to integrate these two levels through interdisciplinary training programs, such as:

- *strategic intelligence and decision-making analysis* courses organized at the “Mihai Viteazul” National Intelligence Academy;
- SRI–MAE–DNSC cooperation for training personnel in the field of cyber diplomacy;
- partnerships with civilian universities for disinformation research (University of Bucharest, SNSPA, “Babeş-Bolyai” University).

This approach, in which the analysis process is doubled by an internal mechanism of self-correction and institutional learning, inspired by complex systems theory (Chandler, 2014), provides flexibility in managing uncertainty and reduces the risk of cognitive errors in the strategic decision-making process.

In conclusion, given the above, at a theoretical level, Romania assimilates models of increasing the resilience of intelligence services in the Euro-Atlantic space, where NATO provides the strategic defense framework and the EU provides the governance and civil cooperation architecture. Overall, Romanian intelligence services are **evolving from reactive security to resilience**, having a solid foundation in the ability to learn and adapt to the security context generated by the hybrid war led by the Russian Federation (Manea, 2021, pp. 52-53).

CONCLUSIONS

The analysis carried out in this scientific article confirms that the **resilience of intelligence services** represents an essential component of the 21st century security architecture, especially in the context of hybrid warfare.

Essentially, **NATO** focuses on interoperability, joint military capabilities and collective exercises, while the **EU** promotes strategic coordination, cyber regulation and societal resilience. NATO and the EU, although starting from distinct institutional paradigms, have converged towards a **common vision**: protecting democratic societies through an intelligence system capable of anticipating, absorbing and adapting to complex shocks. One of the most sensitive issues of intelligence resilience is the **balance between transparency and security**, so while the EU promotes a culture of open governance, NATO and national intelligence structures traditionally operate within a narrow, confidential framework.

To the extent that elements such as trust versus sharing (sometimes certain rivalries limit the exchange of information); legal/constitutional limitations (given by the sovereignty of states); dependence on some private infrastructures

(which sometimes do not comply with the same standards of secrecy/security) will be overcome, the resilience of intelligence services will reach an optimal level for countering hybrid threats that are becoming increasingly complex, by combining multiple types of manifestations (e.g. combining cyberattacks with disinformation).

Romania, located at the intersection of these two systems, manages to build a **mixed resilience** in the field of intelligence services, adapted to its own needs and vulnerabilities. By reforming in relation to NATO and EU standards, Romanian intelligence services have become an active part of information flows, have proven that they have the capacity to adapt institutionally and to develop strategic analysis capabilities and, implicitly, adequate operational resilience to manage the threats of the hybrid war waged by the Russian Federation against the Euro-Atlantic space.

BIBLIOGRAPHY:

1. Administrația Prezidențială (2020). *Strategia Națională de Apărare a Țării pentru perioada 2020–2024. O Românie sigură și prosperă într-o lume marcată de noi provocări*. București, https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_Tarii_2020.pdf, retrieved on 15 October 2025.
2. Blockmans S., Crosson D.M., Paikin Z. (2022). *CEPS Policy Insights*, https://cdn.ceps.eu/wp-content/uploads/2022/03/CEPS-PI2022-14_EU-Strategic-Compass.pdf, retrieved on 14 October 2025.
3. Chandler, D. (2014). *Resilience: The Governance of Complexity*. Routledge.
4. Council of the European Union (2022). *A Strategic Compass for Security and Defence – For a European Union that protects its citizens, values and interests and contributes to international peace and security*, <https://www.consilium.europa.eu/en/policies/strategic-compass/>, retrieved on 12 October 2025.
5. Duchek, S. (2020). *Organizational resilience: A capability-based conceptualization*. Business Research, 13(1), pp. 215-246.
6. ENISA (2023). *ENISA Work Programme 2023*. European Union Agency for Cybersecurity. European Union, <https://www.enisa.europa.eu/publications/corporate-documents/work-programme-2023>, retrieved on 12 October 2025.
7. ENISA (26 June 2025). *NIS2 technical implementation guidance*. European Union Agency for Cybersecurity, <https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance>, retrieved on 10 October 2025.
8. European Commission & High Representative of the Union for Foreign Affairs and Security Policy (2016). *Joint framework on countering hybrid threats: A European Union response*, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016JC0018>, retrieved on 11 October 2025.

9. European Commission (2020). *The EU's cybersecurity strategy for the digital decade*, <https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade>, retrieved on 10 October 2025.
10. European External Action Service (EEAS) (2022). *EU Single Intelligence Analysis Capacity (SIAC): Overview and functions*. Brussels: EEAS, <https://www.eeas.europa.eu>, retrieved on 11 October 2025.
11. European External Action Service (2022). EU Intelligence and Situation Centre (INTCEN): Overview and functions, <https://www.eeas.europa.eu>, retrieved on 10 October 2025.
12. European Union Agency for Cybersecurity (ENISA) (31 January 2023). *The NIS2 Directive: Network and information systems directive 2*, <https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/raising-awareness-campaigns/network-and-information-systems-directive-2-nis2>, retrieved on 10 October 2025.
13. European Union. What is the European Union?, https://op.europa.eu/webpub/com/eu-and-me/en/WHAT_IS_THE_EUROPEAN_UNION.htm, retrieved on 10 octombrie 2025).
14. Galeotti, M. (2016). *Hybrid War or Gibrinaya Voyna? Getting Russia's non-linear military challenge right*. Mayak Intelligence Report.
15. Hamel, G., Välikangas, L. (2003). *The quest for resilience*. Harvard Business Review, 81(9), pp. 52-65
16. Hoffman, F.G. (2007). *Conflict in the 21st Century: The Rise of Hybrid Wars*. Potomac Institute for Policy Studies.
17. Hybrid Centre of Excellence (2021). *Building resilience against hybrid threats: Lessons learned from the Baltic region*. Helsinki: Hybrid CoE.
18. Hybrid Centre of Excellence (2023). *Hybrid influence operations and resilience*. Helsinki: Hybrid CoE.
19. Lengnick-Hall, C.A., Beck, T.E., Lengnick-Hall, M.L. (2011). *Developing a capacity for organizational resilience through strategic human resource management*, in *Human Resource Management Review*, 21(3), <https://doi.org/10.1016/j.hrmr.2010.07.001>, retrieved on 10 October 2025.
20. Linkov, I., Kott, A. (2019). *Fundamentals of cyber resilience: Building a secure and resilient digital society*. Springer.
21. Linkov, I., Trump, B.D. (2019). *The science and practice of resilience*. Springer.
22. Lowenthal, M.M. (2017). *Intelligence: From secrets to policy* (7th ed.). CQ Press.
23. Manea, A. (2021). *Adaptabilitatea serviciilor de informații românești în contextul amenințărilor hibride*. Analize de Securitate, 10(2), pp. 45-63.
24. Mumford, A. (2020). *Ambiguity in hybrid warfare*. Helsinki. The European Centre of Excellence for Countering Hybrid Threats, https://www.hybridcoe.fi/wp-content/uploads/2020/09/202009_Strategic-Analysis24-1.pdf, retrieved on 15 October 2025.

25. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) (2021). *Locked Shields 2021 after-action report*. Tallinn: CCDCOE, retrieved on 15 October 2025.
26. NATO Intelligence Fusion Centre (n.d.). *Who we are/Mission*, <https://web.ifc.bices.org.html>, retrieved on 12 October 2025.
27. NATO StratCom Centre of Excellence (2023). *Resilience in the information environment: Countering hybrid narratives*. Riga: NATO StratCom COE, retrieved on 12 October 2025.
28. NATO, <https://ccdcoe.org/locked-shields>, retrieved on 11 October 2025.
29. NATO, <https://www.act.nato.int/activities/federated-mission-networking.html>, retrieved on 11 October 2025.
30. NATO, [https://www.coemed.org/files/stanags/01_AJP/AJP-01_EDF_V1_E_\(1\)_2437.pdf](https://www.coemed.org/files/stanags/01_AJP/AJP-01_EDF_V1_E_(1)_2437.pdf), retrieved on 11 October 2025.
31. NATO, <https://www.nato.int/en/about-us/organization/nato-structure/resilience-committee>, 7 October 2022, retrieved on 11 October 2025.
32. NATO (2016). *Commitment to enhance resilience* (Warsaw Summit Communiqué, para. 73). North Atlantic Treaty Organization, <https://www.nato.int>, retrieved on 11 October 2025.
33. NATO (2020). *Joint Intelligence, Surveillance and Reconnaissance (JISR)*. Brussels: NATO Public Diplomacy Division, <https://www.nato.int/en/what-we-do/deterrence-and-defence/joint-intelligence-surveillance-and-reconnaissance>, retrieved on 11 October 2025.
34. NATO (2022), [https://www.coemed.org/files/stanags/01_AJP/AJP-01_EDF_V1_E_\(1\)_2437.pdf](https://www.coemed.org/files/stanags/01_AJP/AJP-01_EDF_V1_E_(1)_2437.pdf), retrieved on 12 October 2025.
35. NATO (2022). *Resilience and defence: Strengthening NATO's deterrence and defence posture*. Brussels: NATO.
36. NATO (2024). *Resilience, civil preparedness and Article 3*, https://www.nato.int/cps/en/natohq/topics_132722.htm, retrieved on 10 October 2025.
37. North Atlantic Treaty Organization. *What is NATO?*, <https://www.nato.int/en/what-is-nato.html>, retrieved on 10 October 2025.
38. Popescu, A. (2022). *Evoluții recente în securitatea cibernetică din Europa Centrală și de Est*, in *Revista Română de Studii de Securitate*, 5(2), pp. 45-60.
39. Rathje, S., Navarre, A. (2022). *What Is Societal Resilience?*, AXA Research Fund.
40. Serviciul de Informații Externe (n.d.). *Misiune și cooperare internațională*, <https://www.sie.ro/>, retrieved on 12 October 2025.
41. Serviciul Român de Informații (2023). *Raport de activitate 2022-2023*. București.
42. UE (2019). *Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (Cybersecurity Act)*.

Official Journal of the European Union, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0881>, retrieved on 12 October 2025.

43. Waltzman, R. (2017). *The weaponization of information: The need for cognitive security* (Testimony before the U.S. Senate Armed Services Committee). RAND Corporation, <https://www.rand.org/pubs/testimonies/CT473.html>, retrieved on 12 October 2025.
44. Wardle, C., Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policy making* (p. 16). Council of Europe.

PERFORMANCE PSYCHOLOGY AND STRATEGIC RESILIENCE. MOSAIC

Major Ana-Raluca STANCU

Dr. Diana-Cristiana LUPU

Defence Staff

DOI: 10.55535/RMT.2025.3.25

The article is intended to demonstrate the complementarity of psychological performance and strategic resilience, to present some of the theoretical foundations related to performance and resilience as well as the main evidence-based optimization techniques, and some of the identified applications in strategic fields – military, crisis management, intelligence, space programs, especially considering the current volatile, uncertain, complex and ambiguous contexts, where both sustained focus and flexibility are paramount. To meet these objectives, qualitative research methods are employed, particularly grounded theory, namely an inductive approach meant to allow for the formulation of a new theory, probable but not certain, based on the observed patterns, as well as of further research questions.

Keywords: performance psychology; strategic resilience; VUCA contexts; adaptation;

INTRODUCTION

The fact that contemporary world is undergoing major and fast changes, especially as a result of technological progress, is truism. Against this background, considering the increasingly competitive environment, the concept of performance acquires new and multifaceted characteristics. Moreover, because of the converging challenges that may result in disruptions or even shocks, resilience has become paramount. Within this framework, performance psychology emphasizes the development, mainly through effort and perseverance, of an evolutionary mindset that, in turn, enables individuals, organizations and states to embrace challenges, view setbacks as learning opportunities, adapt in the face of uncertainty, and prosper under such circumstances, which is the essence of strategic resilience. In short, performance psychology provides the tools that support strategic resilience.

In this context, taking into account the fact that there is no standardized definition of the key concepts mentioned in the present paper, namely performance psychology and strategic resilience, we find it useful to provide such definitions as they are presented in the studied literature. Having considered the definitions, the paper is intended to demonstrate the complementarity of psychological performance and strategic resilience, to present some of the theoretical foundations related to performance and resilience as well as the main evidence-based optimization techniques, and some of the identified applications in strategic contexts – military, emergency situations and crisis management, intelligence, space programs. These aspects are expected to test not only the mentioned techniques transformative potential especially in volatile, uncertain, complex and ambiguous (VUCA) contexts, where both sustained focus and flexibility are paramount, but also the theoretical saturation, namely the iterative process of collecting and analysing data in the field. To meet these objectives, qualitative research methods are employed, particularly grounded theory, namely an inductive approach meant to allow for the formulation of a new theory, based on the observed patterns, as well as of further research questions.

TERMINOLOGY

Performance has obviously become the focus in the present highly-competitive environment, broadly denoting how successfully a certain task is achieved. Thus, the concept of **human performance optimization** (HPO) has been developed. It is generally defined as *“the process of applying existing and emerging science and technology to individuals allowing them to reach their biological potential”* (MCDC Project, 2021, p. 10), entailing physical, cognitive and psychological aspects. Moreover, two functional aspects of performance are also suggested, as follows: *“1. Performance as a means to an end – that is, to achieve a particular, measurable result. 2. Performance as an end in itself – that is, to do the work or activity for its own sake”* (Raab et al., 2016, p. 13).

In this context, **performance psychology**, as the name suggests, focuses on the psychological perspective of performance, comprising, according to Nitsch and Hackfort, the psychological fundamentals of performance-oriented activities in various action domains, the psychological transfer effects of performance-oriented activities, in particular with regard to personality development, self-esteem, time management, stress control, communication skills, and the optimization of the capability to achieve demanding mental tasks (Ib., p. 12). Division 47 of the American Psychological Association (APA) provides the following definition: *“Performance psychology is the study and application of psychological principles of human performance to help people consistently perform in the upper range of their capabilities and more thoroughly enjoy the performance process”* (APA, 2019). Performance psychology is thus recognized for its broad appeal, involving domains where the human resource has to meet complex and intense demands, therefore resilience becomes a necessity to be defined.

Resilience as a domain of study was first broadly defined in the 1970s as the capacity to maintain health, or to reach adaptive outcomes, even in the presence of adversity (Garmezy, 1974, pp. 74-98). In line with the initial conceptualization, APA defines **(psychological) resilience** as *“the process and outcome of successfully adapting to difficult or challenging life experiences, especially through mental, emotional, and behavioral flexibility and adjustment to external and internal demands. A number of factors contribute to how well people adapt to adversities, predominant among them (a) the ways in which individuals view and engage with the world, (b) the availability and quality of social resources, and (c) specific coping strategies”* (APA, Glossary, <https://www.apa.org/topics/resilience>). It naturally

follows that resilience depends on individual characteristics as well as on the environment and the resources.

Considering that it somehow measures the way people adapt to adversities and combining it with the increasingly challenging environment, the resilience-related research has become the focus of business and international organisations as well. Thus, in 2020, especially in the context of the COVID-19 pandemic, the European Commission (EC) established the *Recovery and Resilience Task Force (RECOVER)*. It was operational until 1 February 2025 when its responsibilities were taken over by the *Reform and Investment Task Force* (EC, https://commission.europa.eu/about/departments-and-executive-agencies/recovery-and-resilience-task-force_en). In this context, the EU Strategic Foresight Report (2020) places resilience, defined as “the ability not only to withstand and cope with challenges but also to undergo transitions, in a sustainable, fair, and democratic manner” (JRC, Resilience, 2020), as a new compass for EU policies. Thus, “building a more resilient society calls for strengthening the mechanisms of shock absorption and enhancing the capacity for adaptation and transformation (...), (entailing) four interrelated dimensions: social and economic, geopolitical, green, and digital” (Ib.), the path to the strategic dimension of resilience being open.

Strategic resilience is a concept originally used in business, considering the environment complexity, competitiveness and low level of predictability. In this context, strategic resilience is defined as “the capacity of a business to endure, adapt, and thrive amidst external pressures or changes without compromising its strategic objectives and integrity” (Study Smarter, 2024). Thus, leadership agility, cultural flexibility, robust relationships and scenario planning are considered key components of strategic resilience (Ib.). With a focus on the organization, “strategic resilience refers to the ability of an organization to effectively pursue opportunities in a competitive environment, while also being able to adjust to change without experiencing any financial or other crises” (Välikangas, 2016). In a broader context, strategic resilience can be seen as “the practice of thinking forward while leading through present turbulence – adapting to difficult operating circumstances while looking beyond current conditions to keep focused on the horizon” (Coffaro, 2020) in an operating environment characterised by dynamic uncertainty.

Having clarified the working definitions, we will present some of the most influential theoretical foundations related to performance and resilience.

THEORETICAL FOUNDATIONS

The **Yerkes–Dodson law** of arousal and performance, formulated in 1908, postulates the optimal level of mental arousal, like excitement or alertness. In a very briefly presentation, the psychological principle tested by the law shows that low arousal leads to boredom and poor results, moderate arousal boosts focus and efficiency, while overarousal results in stress, mistakes and thus decreasing performance (*figure 1*). However, the law should be considered only as a general guideline, especially taking into account the fact that the original experiment involved mice and punishment in the event of failing to accomplish the given task, on the one hand, and the individual differences and situational factors, on the other hand. Thus, modern research has shown that the curve can vary across individuals and contexts (Nickerson, 2025).

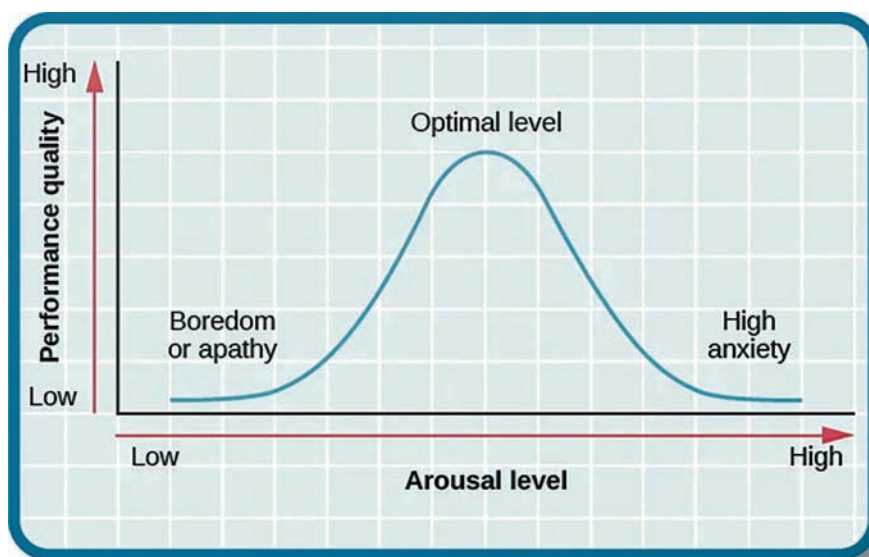


Figure 1: Yerkes-Dodson Law of Arousal and Performance (Nickerson, 2025)

Cognitive Load Theory, developed by educational psychologist John Sweller in the 1980s, has used elements of human cognition to generate instructional effects, in the sense of optimizing intellectual performance, in the context of a study on problem solving. Thus, *“cognitive load is generally considered a construct representing the load that performing a particular task imposes on the cognitive system. It can be conceptualized as a task-based dimension (i.e., mental load) and a learner-based dimension (i.e., mental effort), both of which affect performance. (...).*

Performance refers to the associated learner's performance" (Sweller et al., 1998, p. 266). In this context, schemas are considered to be examples of sophisticated rules. Automated schemas allow for both fluid performance on familiar tasks and levels of performance on unfamiliar aspects that otherwise might be impossible. In short, cognitive load theory assumes that all information that must be processed in working memory is part of an interactivity continuum. The low element interactivity is associated with low intrinsic cognitive load. In contrast, the high element interactivity materials require them to be processed simultaneously in working memory resulting in a high intrinsic cognitive load. Learning reduces that load by embedding interacting elements in schemas. (Ib., pp. 257, 258, 290).

Connecting the exposed theories related to learning and performance with the concept of resilience, which entails enhancing the capacity for adaptation and transformation, we consider it important to present a theory, formulated by Hans Selye in the 1950s, describing the body response to stressors, be they negative or positive, namely the **General Adaptation Syndrome (GAS)**. The theory states that the body response to stressors undergoes three stages: alarm reaction (fight-or-flight), resistance (the body recovers), and exhaustion (fatigue and burnout) (Selye, 1977, p. 85). In time, and in sync with the social and technological progress, associated concepts have been developed, such as the *"pathology of progress"*, especially in connection to the increasing levels of mental stress, fatigue, and traumatic neurosis among industrial workers and soldiers. In addition, the concept of *"diseases of adaption"* was introduced, mainly related to the role of hormones in mediating resistance to stress, which has been promoted as a new language of disease (Rosenberg, 1998, pp. 714-730).

RESILIENCE FRAMEWORKS

In line with resilience conceptualization, many frameworks have been developed, intended not only to provide a systematic and strategic structure to the concept but also to identify and build the capacities needed to respond to adversity and even to prevent or adapt to it. Among them, we will briefly present the following: BCI, ICOR, Fraunhofer EMI, as well as Merkt & Ziehr Strategic Resilience Model.

BCI Framework has been developed by a group of experts belonging to the Business Continuity Institute (BCI), offering a robust structure for organizations to enhance resilience in a systematic manner (BCI, 1.0). In this context, a set of eight core principles for all resilience development and management activities within an organization have been established as follows: • Resilience is led from the top;

- It requires clear direction on purpose, objectives and required outcomes;
 - It requires a comprehensive understanding of the organization's current state;
 - A risk-based approach is necessary;
 - Resilience is coherent and collaborative;
 - It incorporates a defined set of strategies and related operational solutions;
 - Being able to adapt is a characteristic of resilience;
 - It is always cyclical (Ib.)
- (figure 2).



Figure 2: The Resilience Framework Cycle (Ib.)

ICOR's Organizational Resilience Framework has been developed by the International Consortium for Organizational Resilience (ICOR). In this particular framework, twelve management disciplines that effectively manage risk have been identified (ICOR) (figure 3). Moreover, accepting the fact that there are few situations in which a single strategy or solution can make an organization resilient, some other enhancement approaches are presented, comprising managing risk in a coordinated manner, building a healthy organizational culture, and increasing the capabilities to adapt and manage change (Ib.).



Figure 3: ICOR Management Disciplines (Ib.)

Fraunhofer EMI resilience cycle gravitates to the *strategic planning of resilience*, especially in the case of technical systems, a process subdivided in five phases – Prepare, Prevent, Protect, Respond, Recover, which constitute the cycle (Fraunhofer EMI).

Merkt & Ziehr Strategic Resilience Model connects strategic resilience to human performance in the context of science and education (Ziehr, Merkt, 2024) (figure 4).

The mentioned model connects the psychological, physical and cognitive aspects, showing that the capability to act depends on the interaction between the three, especially at the individual level, as well as on the context. It is thus shown that, in special operational situations, such as the military, common resilience models may reach their limits to include the strategic resilience approach that focuses on overcoming crisis situations, preventing them, and making dynamic decisions, allowing for developing a strategy to improve effectiveness in special operational situations. Such multidimensional consideration can help actors to improve their skills in terms of *human performance optimization* and *human performance strategic resilience*. (Ib.).

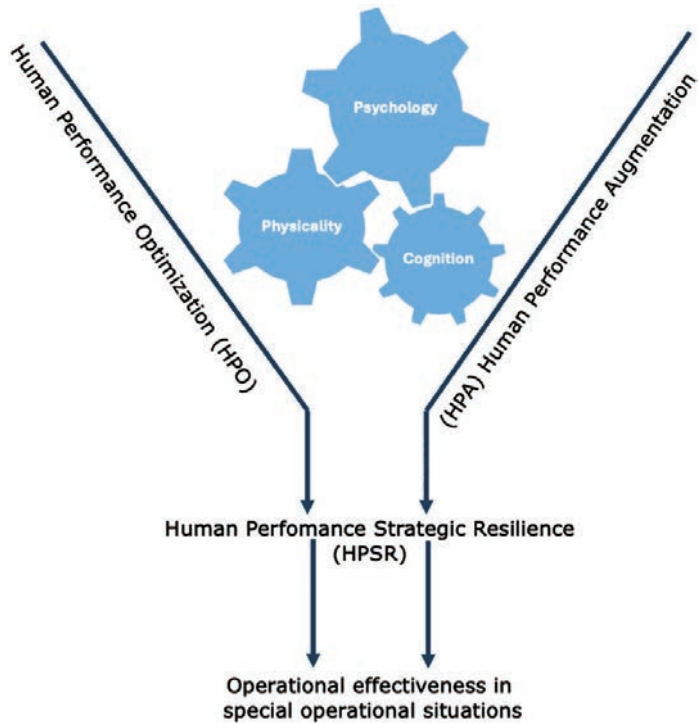


Figure 4: Model of strategic resilience in human performance (lb.)

In this context, mention should be made that Human Performance Optimization (HPO), more often than not based on AI-driven cognitive training programs, comprises Human Performance Modification – HPM, Human Performance Augmentation – HPA; Human Performance Enhancement – HPE; and Human Performance Restoration – HPR. We only mention these aspects in the present paper, considering them as future research directions that exceed the set objectives. Consequently, focusing on the topic, we will retain only the performance psychology-related aspects and we will briefly present some enhancement techniques found in the studied literature.

ENHANCEMENT/OPTIMIZATION TECHNIQUES

The tasks associated with the military require achieving not only physical but also mental readiness. In this context, holistic approaches have been adopted in the military too. For instance, one of the US Army human resource priorities is to develop a more comprehensive understanding of the factors related to readiness, thus insights into optimizing troops’ performance being provided. In this regard, some of the identified strategies associated with self-regulation and optimal performance

entail skills such as goal setting, imagery, attentional control and thought control, all of them being especially necessary for performance optimization and cognitive function in high-stress environments such as the military (Leone et al., 2025).

In this context, the Center for Army Lessons Learned released the US Army Holistic Health and Fitness (H2F) Handbook (Faulkenberry et al., 2023). It is presented as able to change the culture of health and fitness in the Army to help meet the demands of modern combat. *“H2F is an enterprise-wide readiness system that combines all aspects of physical and non-physical human performance optimization under a single governance structure to enable commanders to improve Soldier health and fitness. This system encompasses five domains: 1. Mental Readiness – The ability to meet the mental demands of combat or duty position; 2. Sleep Readiness – The ability to implement the requisite sleep principles and behaviors to support optimal brain function; 3. Nutritional Readiness – The ability to recognize, select, and consume the requisite food and drink to meet the physical and non-physical demands of any duty or combat; 4. Spiritual Readiness – The development of personal qualities needed to sustain a person in times of stress, hardship, and tragedy; 5. Physical Readiness – The ability to meet the physical demands of any duty or combat and accomplish the mission”* (Ib., p. 1).

In what follows we will provide a brief description of some of the identified techniques meant to enhance performance.

❖ *Goal setting* is a performance psychology technique designed to enhance achievement by providing a sense of direction and desired target outcome. All of us and especially the military need the ability to persevere and perform under both immediate danger and long-term stress, not only on the job but also at home. For instance, in the Naval Special Warfare Community, *“Warrior Toughness (WT) is considered to be a holistic human performance skillset that enhances the toughness of the Sailors with a focus on the pursuit of peak performance, which emphasizes the development of toughness in the mind, body, and soul. WT combines performance psychology skills with character development, and teaches the Warrior Mindset”* (Naval Education and Training Command, Glossary of Terms). In terms of goal setting, the same source mentions the fact that Outcome Goals (long term vision statements) should be aligned with Performance Goals (specific longer-term goals) and Process Goals (specific short-term goals), and Performance Goals should be SMART (Specific, Measurable, Attainable, Relevant, and Time-based) (Ib.).

❖ *Visualization/Imagery* is defined as not only a cognitive process fundamental to motor learning and performance but also a mental technique that can be refined

with practice and utilized in many ways to enhance performance (Cumming, Williams, 2012, p. 213). There are five main characteristics of the imagery process: modality, perspective, angle, agency, and deliberation (Ib., p. 214). It has been demonstrated that imagery shares neural and behavioural similarity to the genuine experience. Research has shown that the effects on performance enhancement can occur both immediately and over time, due to changes in neural plasticity, on condition areas of brain activation during imagery are as similar as possible to those active during execution of the desired outcome. That is the reason why different methods for enhancing imagery ability, related to cognitive neuroscience evidence, have been proposed, such as those based on the Physical, Environment, Task, Timing, Learning, Emotion, and Perspective (PETTLEP) model (Ib., pp. 219-220).

❖ *Mindfulness* is a performance psychology technique defined as present moment awareness, which may entail both the self and the situation. The technique can help prevent not only the state of being overwhelmed but also distractions, therefore resulting in increasing focus, especially in high-stress situations. In the introduction of the Naval War College cognitive fitness and mindful resilience initiative, it is specified that *“Mindfulness is often thought of as a way to promote emotional well-being and resilience and to reduce stress. (...), research has also indicated that it can strengthen areas of cognitive performance. (...) Findings indicate that mindfulness practice can improve working memory, sustained attention, cognitive flexibility, empathy, and decision making. (...) these outcomes point to a particular benefit for members of high-stress occupations such as the military and for leaders at all levels (...)”* (US Naval War College, 2025).

❖ *Biofeedback & Heart Rate Variability training* is an exercise related to mindfulness technique, designed to teach people to better observe physic sensations objectively. In the documented case of Sailors, the exercise, performed by systematically focusing on each part of the body and then noticing whatever sensations are there in a non-judgmental manner, will help train them to be prepared to perform in uncomfortable environments. *“The broader purpose is to give Sailors an opportunity to practice refocusing on the here and now when their minds wander”* (Naval Education and Training Command, Glossary of Terms).

❖ *Reframing* is a performance psychology technique that entails a process of reflection meant to help people develop resilience and adaptability. More precisely, it is related to the fear of making mistakes, especially considering the cultural perspective in which people are taught to aim for perfection, which can lead to anxiety about failure, creating a sense of pressure. However, by reframing errors,

people can find the purpose of mistakes and can focus on processes or actions that are within their control (Condor Performance, 2025).

❖ *Mental rehearsal* is a performance psychology technique that resembles a virtual reality practice session in the mind, thus helping to prepare for tasks that are stressful and/or high risk. The documented exercise for Sailors, performed as a group, consists of *“a written script that is read aloud, allowing them to mentally rehearse in a manner that is both vivid (using all senses) and controlled (only rehearsing desired outcomes). The same visualization process can also be used by Sailors individually in the moments leading up to the actual stressful and/or high-risk situation”* (Naval Education and Training Command, Glossary of Terms).

❖ *Building support systems* is another documented performance enhancement technique. Thus, it has been demonstrated that, in the case of athletes, psychosocial support, defined as encompassing both sporting figures (trainers, teammates etc.) and non-sporting individuals (family, friends etc.), is crucial for fostering resilience, protective resources, and coping mechanisms. The provided support may include emotional reinforcement, boosting self-esteem, adding information, as well as tangible assistance, studies having shown a positive correlation between psychosocial support and improved performance and better resilience (Lane, 2024).

APPLICATIONS IN STRATEGIC CONTEXTS

In the late 1980s, with the end of the Cold War, it was assumed that the global system ceased to be a bipolar one, which resulted in increasing volatility, uncertainty, complexity and ambiguity of general conditions and situations (Bennis, Nanus, 1985). Thus, based on the acronym for the mentioned characteristics, the concept of VUCA context is considered to be coined by the US Army War College, by introducing it in the curriculum in 1987 (US Army Heritage and Education Center, 2019). Moreover, in 1991, related to the US Army War College experience, strategic leadership was defined within a *“volatile, uncertain, complex and ambiguous global environment...”* (Barber, 1992, p. 8).

In general terms, the VUCA framework entails tools, processes and strategies related to change, challenges, risks, anticipation, preparation, prevention, protection, planning, decision-making, response, improvement, learning, adaptation, recovery, which are all elements of commonality for the presented resilience framework cycles, performance psychology enhancement techniques, and strategic management. Moreover, VUCA, to which terms like chaos, nonlinearity, paradox, delayed feedback and information flow have been suggested to add over time, serves as a roadmap

for different organizations to develop strategies for readiness, foresight, adaptation, proactive intervention and recovery in complex and extremely requiring situations.

In this context, we will provide some examples of the identified and already implemented programs meant to foster resilience in domains considered strategic, such as the military, emergency situations and crisis management, intelligence, and space programs.

Military

The US Army Master Resilience Trainer (MRT) course provides face-to-face resilience training, being one of the foundational pillars of the Comprehensive Soldier Fitness program. The curriculum includes three components: preparation, based on the Penn Resilience Program (PRP) curriculum as well as on other empirically validated interventions from positive psychology; sustainment, developed by researchers at the Walter Reed Army Institute of Research; and enhancement, developed by sports psychologists within the United States Military Academy at West Point, teaching personal and professional skills that maximize individual performance (Reivich et al., 2011, p. 25).

Basic Underwater Demolition/SEAL (BUD/S) training is a very demanding program that “requires an iron will, exceptional determination, and resilience to succeed” (as it) “pushes candidates to their limits and beyond, testing physical endurance, mental resilience, and team spirit like no other military training in the world (...) Imagine being pushed to your absolute limit (...) then being asked to push even harder. That’s what BUD/S Training feels like every single day”. (Navy Seal Military News, <https://www.navyseal.com/bud-s/>).

Expanded Operational Stress Control (E-OSC) is part of the Navy’s Culture of Excellence, designed to enhance resilience, readiness, and stress navigation across the fleet. E-OSC employs evidence-based practices to build toughness and resilience through peer-to-peer support, self-care, and connectedness. The program began in 2008, evolving and incorporating advanced resilience concepts not only to address the changing needs of sailors and commands, but also adapted to caregivers in the Navy Medicine as well as to fleet and family support centres. Moreover, the program introduces the *Expanded Stress Continuum*, which recognizes stress as a tool for growth, with defined states ranging from Idle (lethargic or recovering), to Ready (manageable stress), Reacting (temporary stress), Injured (need for outside support) and Ill (requiring medical attention) (My Navy HR, https://www.mynavyhr.navy.mil/Support-Services/Culture-Resilience/Warrior-Toughness/E-OSC_SOM/).

NATO Resilience Reference Curriculum

Based on the idea expressed in NATO 2022 Strategic Concept, namely that *“We will pursue a more robust, integrated and coherent approach to building national and Alliance-wide resilience against military and non-military threats and challenges to our security, as a national responsibility and a collective commitment rooted in Article 3 of the North Atlantic Treaty”* (Para 26, p. 7), the Resilience Reference Curriculum was developed and released in January 2025, as a guiding framework for developing courses, study programs and trainings on the topic (NATO Resilience Reference Curriculum, 2025, p. 3). Considering resilience from the individual to the multinational and showing the interrelations between all the levels, the Curriculum addresses strategies in managing and sustaining individual resilience, covering tools for both the individual to manage and sustain own resilience and for leaders tasked with managing and sustaining the others resilience, mentioning the following as foundations: *“meaning and purpose, mindfulness, physical health, mental/emotional health, a growth mindset, and social support”* (ib., p. 86).

Emergency Situations and Crisis Management

Research in the area of special operation situations often focuses on the human performance cluster. An example is the Unit of *Applied Research 18_RECESS* (18_ Research and Education Center for Extraordinary Tactical Situations and Strategically Resilience) at the Department of Disaster Prevention and Crisis Management at Fresenius University of Applied Sciences in Idstein, which pursues the adaptation of existing resilience models to special operation situations in line with the definition of strategic resilience, focusing on training strategic resilience (Ziehr, Merkt, 2024). In this regard, there are several ongoing research projects, involving both civilians and military, mainly related to the possibility to train several domains of strategic resilience via problem-oriented intervention (POH), considering the three axes of strategic resilience, namely psychological, physiological and cognitive resilience, as well as the examination of robustness or performance in more detail, focusing on human performance, including HPM, HPA, HPE, HPD, HPR. All in all, different dimensions of resilience are considered, pertaining to natural sciences, humanities, social sciences, medicine, psychology and spirituality, to capture resilience multidimensionally and derive training options to increase the robustness of individuals in the context of human performance optimization in crises and disasters (ib.).

Intelligence

The *Multimodal Objective Sensing to Assess Individuals with Context (MOSAIC)* program, running from July 2017 to December 2020, was aimed to advance the Intelligence Community's ability to evaluate an individual's psychological drivers, cognitive abilities, and mental resilience to predict their job performance. Considering the limitations of current assessment tools, MOSAIC is the first program that uses *"advances in mobile, wearable, and environmental sensors to develop continuous assessments of an individual's professional performance, and psychological and physiological well-being throughout their career. In phase 1 of the program, performers collected real-world, contextually rich data from sensors, mobile apps, and software from volunteer participants. In phase 2 of the program, performers made their rich data sets available to the research community"* (IARPA). One of the accomplishments of the program was that it established standardized formats and guidelines for curating complex multimodal data. Curated datasets are available to government partners as well as the broader research community via links to performers' data repositories accessible through MOSAIC's Open (Ib.).

Space programs

The *Stress Management and Resilience Training for Optimal Performance (SMART-OP)* project, running between 2008 and 2012, was based on cognitive-behavioural therapy (CBT), including education about stress, and interactive training exercises that taught users to monitor stress, regulate emotions and relax, think flexibly, be realistic, and take effective action to deal with stressors. Its content could be modified to target those working in challenging environments (e.g., astronauts, military, and flight controllers) and disseminated widely via computer, tablet, or smartphone. In fact, it is a *"computer-based, self-guided multimedia, interactive, evidence-based stress management and resilience training program"* (NASA), considering that stress plays a significant etiological role in the onset of many physical and psychiatric disorders (Ib.).

MINDFUL-ICE, a study conducted in a high-fidelity analogue environment, sometimes defined as the *"White Mars"*, namely the Concordia station, a research base located in Antarctica, investigated mindfulness as a predictor for lower stress over the course of long-term missions in isolated, confined, and extreme environments (Pagnini et al., 2024). In the same vein, *"A Quick Mindfulness Training for an Isolated and Confined Environment"* (*MINDFUL-ICE II*) is a program supported by the European Space Agency, the French Polar Institute Paul-Émile Victor, and the Programma Nazionale di Ricerche in Antartide to go deeper into the research

of practices such as diaphragmatic breathing, progressive muscle relaxation and mindfulness in order to integrate them into astronauts' training to help them manage the ongoing psychological demands of space missions. These methods are not only non-invasive but also easy to practice, making them ideal for space, where time and resources are limited (Pagnini, 2024).

THEORY DEVELOPMENT

Considering the grounded theory as the main research method employed in developing the paper, which entails inductive reasoning, we will combine the above-presented observations, the identified patterns and their coding with experiential information to formulate a theory that is intended to broaden the framework of performance psychology and strategic resilience complementarity. In this way, a hypothesis and new research questions will be generated, which we expect to be topics addressed in further research endeavours. Mention should be made, in this context, that, taking into account the limitations stemmed from the impossibility to observe every possible instance, the developed theory is a probable but not a certain one.

All these considered, resilience frameworks, be they related to individuals, as well as national and multinational business, organisations or even states, have certain aspects in common as follows: awareness, assessment, building capacity, adaptability, agility, integrated approach, which indicates the multidimensional trait of resilience. By adding the ability to endure, adapt and thrive in changing and requiring environments, keeping the focus and meeting the set objectives, to the mentioned characteristics, the strategic dimension of resilience is outlined. Moreover, the complementarity of strategic resilience and performance psychology as well as the interdependence between the individual, the environment and available resources are emphasized.

Under these circumstances, based on the patterns identified in the presented performance and resilience-related models, developed, experimented, budgeted and tested, involving not only subject matter experts but also practitioners, we advance the hypothesis that these issues are not completely new, even if the terminology may be different. It is somehow normal, considering that, since ancient times, human beings have been confronted with struggles, changes and choices. Yet, the human race has managed to survive in one way or another. Nevertheless, it may mean gain or loss for some social organisations and individuals. Therefore, the question arises whether a win-win solution could be possible for everyone in the long run, which has been coined utopia so far. Utopia is defined as an ideal

society based on unrealistic perfection. Concurrently, the term eutopia has been also introduced, meaning a desirable and achievable society that focuses on continuous improvement rather than perfection, which seems to be a more realistic perspective, fostering a sense of attainable progress and promoting resilience.

In this context, the above-presented models of resilience revolve around the concept of cyclicity, emphasising preparation, prevention, protection, response and recovering as main stages. In addition, and in connection to performance psychology, Merkt & Ziehr model considers HPM, HPA, HPE and HPR as subunits of HPO, taking into account the rapid and even astonishing technological advances. Moreover, the mentioned theoretical foundations emphasize the concepts of optimal level of arousal, mental load and effort, adaptation syndrome with the associated pathology, as well as that of interactivity continuum. Furthermore, most of the presented performance enhancement techniques and applications are holistic, entailing mind, body and soul, which aligns with the principles of resilient thought, iterative and sustainable in nature, encouraging integration of diverse systems and approaches.

By and large, the survival of the human species over thousands and thousands of years may indicate an underlying universal guiding principle that is likely to be connected to the knowledge and development of the self, which maintains the existence and evolution of the body, shaping the energy of life in matter and covering the entire spectrum of frequencies. In this context, it can be said that the appropriate response to challenges should be sought within. Thus, one of the steps to follow in building resilience is for the subject to know the basis of own being, that is to recognize all innate capacities, those acquired through experience, as well as dormant ones that are waiting to be unveiled and used through one's own effort. Mention should be made, in this regard, that there are psychological tests that can be applied for self-knowledge.

However, from a physiological and psychological perspective, the living cell is made to function healthily in a certain frequency range. Under these circumstances, the question then arises related to the level of challenge in the environment that can be processed and integrated, which is, in fact, resilience. If, in a too challenging environment, only rational consciousness can develop, which is intelligence and logic, not emotion, a community cannot thrive. Nevertheless, resilience and performance models highlight the concept of community, involving people who see solutions in a much deeper way, who are loyal, and thus inspiring and supportive. Therefore, an organization, no matter its size and purpose, succeeds through its valuable people who naturally have the mentality of winners through themselves

and thus attract the gain for the organization. If the members of the organization do not progress through their decisions but decline, then, in the long run, the organization will only win through deception. There may be organizations that can choose to take deception to the level of art and continue to win by manipulating and distorting the reality.

Therefore, one might ask what is the level of “*healthy*” resilience in an increasingly “*unhealthy*” environment, considering, in terms of performance, that the desire to be seen as a professional, to accomplish as many projects as possible for the organization, to be appreciated for the achievements can be seen as human nature, especially in the current social and cultural context, focused on competitiveness. Under such circumstances, the interconnection between biological, social and psychological factors in human life, which substantiates the holistic approach to resilience, is once more emphasized.

INSTEAD OF CONCLUSION

All the presented aspects considered, there is still a lingering question: Have we been designed as human beings or as human doers, achievers or fixers?

BIBLIOGRAPHY:

1. American Psychological Association (26 July 2019). *Coaching Elite Performers. The Role of Performance Psychology*, <https://www.apa.org/pubs/highlights/spotlight/issue-145>, retrieved on 17 September 2025.
2. American Psychological Association. Glossary, <https://www.apa.org/topics/resilience>, retrieved on 17 September 2025.
3. Barber, H. F. (1992). *Developing Strategic Leadership: The US Army War College Experience*. Journal of Management Development 11, no. 6, pp. 4-12.
4. Bennis, W., Nanus, B. (1985). *Leaders: Strategies for Taking Charge*. New York: Harper & Row.
5. BCI Resilience Framework, UK, <https://www.thebci.org/certification-training/resilience-framework.html>, retrieved on 19 September 2025.
6. Coffaro, D. (27 July 2020). *Strategic Resilience. Lead Change*, <https://leadchangegroup.com/strategic-resilience/>, retrieved on 18 September 2025.
7. Colberg, T. (2022). *Strategic Resilience: A systematic review of leading literature*. Journal of Business Management, Vol. 20. DOI: 10.32025/JBM22004.
8. Condor Performance (8 January 2025). *Reframing Mistakes and Errors*, <https://condorperformance.com/reframing-mistakes/>, retrieved on 23 September 2025.
9. Cumming, J., Williams, S.E. (January 2012). *The Role of Imagery in Performance*. In *Handbook of Sport and Performance Psychology*, pp. 213-232, Murphy, S. (ed.), Oxford University Press, https://www.researchgate.net/publication/267749244_The_Role_of_Imagery_in_Performance, retrieved on 22 September 2025.
10. European Commission, Recovery and Resilience Task Force (16 August 2020), https://commission.europa.eu/about/departments-and-executive-agencies/recovery-and-resilience-task-force_en, retrieved on 17 September 2025.

11. European Commission, The Joint Research Centre: EU Science Hub (2020), Resilience, https://joint-research-centre.ec.europa.eu/projects-and-activities/resilience_en, retrieved on 17 September 2025.
12. Faulkenberry, J.B., COL, Mansfield, A.J., Cajina, J. (2023). *US Army Holistic Health and Fitness Handbook*. Center for Army Lessons Learned, Fort Leavenworth, <https://api.army.mil/e2/c/downloads/2023/06/05/25e44ff1/23-06-784-holistic-health-and-fitness-handbook-jun-23-public-release-1.pdf>, retrieved on 22 September 2025.
13. Fraunhofer EMI, <https://www.fraunhofer.de/en/research/current-research/archive/safeguarding-critical-infrastructure.html>, retrieved on 19 September 2025.
14. Garmezy, N. (1974). The study of competence in children at risk for severe psychopathology. In Anthony E. J. & Koupernik C. (eds.), *The child in his family: Children at psychiatric risk: III* (pp. 77–98). New York: Wiley.
15. IARPA (Intelligence Advanced Research Projects Activity). Mosaic Program. <https://www.iarpa.gov/research-programs/mosaic>, retrieved on 26 September 2025.
16. ICOR Resilience Framework, <https://www.build-resilience.org/organizational-resilience-framework.php>, retrieved on 19 September 2025.
17. Lane, S. (December 2024). It's people that make the difference: Understanding the significance of psychosocial support for professional athletes. *Mental Health&Prevention*, vol. 36, 200364, <https://www.sciencedirect.com/science/article/pii/S2212657024000461>, retrieved on 23 September 2025.
18. Leone, G.E., Stodden, D.F., Abrams, T.C., Sacko, R.S., Terlizzi, B., Monsma, E. (August 2025). *Psychological Skill Strategies and Physical Performance Implications for Military Readiness*. In *Military Review*, The Professional Journal of the US Army, Army University Press, <https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2025-OLE/Psychological-Skill/>, retrieved on 22 September 2025.
19. Maurer, A. (ed.) (2016). *New Perspectives on Resilience in Socio-Economic Spheres*, Springer VS, https://www.academia.edu/69757146/New_Perspectives_on_Resilience_in_Socio_Economic_Spheres, retrieved on 19 September 2025.
20. Multinational Capability Development Campaign (MCDC) Project (22 March 2021). Project Lead: Cdr Dr. Christian Haggemiller, German Institute for Defence and Strategic Studies, Human Performance Optimization and Enhancement, https://gids-hamburg.de/wp-content/uploads/2021/04/2021-03-22_MCDC_HPEO_Project_Report_final-1.pdf, p. 10, retrieved on 17 September 2025.
21. NASA Human Research Program SMART-OP, <https://techport.nasa.gov/projects/23223>, retrieved on 26 September 2025.
22. NATO Strategic Concept (2022), https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf, retrieved on 26 September 2025.
23. NATO Resilience Reference Curriculum (January 2025), https://www.nato.int/nato_static_fl2014/assets/pdf/2025/2/pdf/DEEP-resilience-reference-curriculum.pdf, retrieved on 26 September 2025.
24. Naval Education Training Command. Glossary of Terms. Warrior Toughness, <https://www.netc.navy.mil/Warrior-Toughness/>, retrieved on 22 September 2025.
25. Navy Seal Military News, <https://www.navyseal.com/bud-s/>, retrieved on 23 September 2025.
26. Nickerson, C. (14 August 2025), *The Yerkes-Dodson Law*. Simple Psychology, <https://www.simplypsychology.org/what-is-the-yerkes-dodson-law.html>, retrieved on 18 September 2025.

27. Nitsch, J.R., Hackfort, D. (2016). *Theoretical Framework of Performance Psychology: An Action Theory Perspective*. In Raab, M., Lobinger, B., Hoffmann, S., Pizzera, A., Laborde, S., (eds.), (2016). *Performance Psychology. Perception, Action, Cognition, and Emotion*. Elsevier Inc., pp. 12, 13, https://www.dshs-koeln.de/fileadmin/redaktion/Institute/Psychologisches_Institut/Juergen_Nitsch_Uploads/Nitsch_Hackfort_2016_Performance_Psychology.pdf, retrieved on 19 September 2025.
28. Pagnini, F., Thoolen, S., Smith, N., van Ombergen, A., Grosso, F., Langer, E., Phillip, D. (March 2024). *Mindfulness disposition as a protective factor against stress in Antarctica: A potential countermeasure for long-duration spaceflight?* In *Journal of Environmental Psychology*, vol. 94, Elsevier, <https://www.sciencedirect.com/science/article/pii/S0272494424000276>, retrieved on 26 September 2025.
29. Pagnini, F. (October 2024). *Supporting the Mind in Space: Psychological Tools for Long-Duration Missions*. In *Interactive Journal of Medical Research*, <https://pmc.ncbi.nlm.nih.gov/articles/PMC11499714/>, retrieved on 26 September 2025.
30. Reivich, K.J., Seligman, M., E.P., McBride, S. (January 2011). *Master Resilience Training in the U.S. Army*, *American Psychologist*, American Psychological Association, vol. 66, no. 1, pp. 25–34, <https://ppc.sas.upenn.edu/sites/default/files/mrtinarmyjan2011.pdf>, retrieved on 23 September 2025.
31. Rosenberg, C. E. (1988). *Pathologies of Progress: The Idea of Civilization as Risk*. In *Bulletin of the History of Medicine*, Winter 72(4), pp. 714–730, <https://pubmed.ncbi.nlm.nih.gov/9879125/>, retrieved on 19 September 2025.
32. Selye, H. (1977). *The Stress of My Life*. Toronto: McClelland and Stewart, p. 85.
33. Study Smarter, UK (17 September 2024). *Business Studies. Strategic Resilience: Framework and Meaning*, <https://www.studysmarter.co.uk/explanations/business-studies/operational-management/strategic-resilience/>, retrieved on 18 September 2025.
34. Sweller, J.; van Merriënboer, J. J. G.; Paas, F. G. W. C. (1998). *Cognitive Architecture and Instructional Design*. In *Educational Psychology Review*, 10 (3), pp. 251–296. doi:10.1023/A:1022193728205. S2CID 127506, https://www.researchgate.net/publication/200772805_Cognitive_Architecture_and_Instructional_Design, retrieved on 18 September 2025.
35. US Army Heritage and Education Center (7 May 2019). *Who first originated the term VUCA (Volatility, Uncertainty, Complexity and Ambiguity)?*, <https://web.archive.org/web/20210602145018/https://usawc.libanswers.com/faq/84869>, retrieved on 23 September 2025.
36. US Naval War College (28-30 July 2025). *Lectures of Opportunity: “Cognitive Fitness and Mindful Resilience at the Naval War College”*, <https://usnwc.edu/News-and-Events/Events/LOO-2024-Cognitive-Fitness-and-Mindful-Resilience-at-the-Naval-War-College>, retrieved on 23 September 2025.
37. Välikangas, L. (July 2016). *Strategic Resilience*. In *The Palgrave Encyclopedia of Strategic Management*, pp. 1-4, https://www.researchgate.net/publication/311907776_Strategic_Resilience, retrieved on 18 September 2025.
38. Ziehr, S., Merkt, P.H. (2024). *Strategic Resilience in Human Performance in the Context of Science and Education – perspective*. *Front. Psychiatry* 15:1410296, https://www.researchgate.net/publication/380154449_Strategic_resilience_in_human_performance_in_the_context_of_science_and_education_-_perspective, retrieved on 19 September 2025.

THE BLUE BASTION: THE DANUBE AS A RESILIENCE LINE – PRELIMINARY CONSIDERATIONS IN NATIONAL DEFENCE ARCHITECTURE –

Lieutenant Claudiu Andrei CERCHIA, BEng

*67th Riverine Gunboat Squadron "Comandor Virgil Alexandru Dragalina",
Romanian Naval Forces*

DOI: 10.55535/RMT.2025.3.26

In the context of recent developments in the regional and global security environment, the Danube stands out as a strategic element of major importance for Romania. Positioned at the intersection of Europe's commercial, energy, and military corridors, the river plays a vital role both in supporting national resilience and in strengthening collective security within NATO and the European Union. Its dual nature – as a natural barrier and a mobility axis – turns it into a bastion of defence against both conventional and hybrid threats. This study examines how the Danube contributes to the architecture of national defence through the integration of civilian and military capabilities, the protection of critical infrastructure, and rapid adaptation to new forms of aggression. The proposed analysis combines the theoretical perspective of military art with operational lessons drawn from recent conflicts, highlighting the need for a proactive, coordinated, and multidimensional approach to managing the Danube region.

Keywords: strategic resilience; national defence; hybrid security; critical infrastructure; international cooperation;

INTRODUCTION

The dramatic changes in the international security environment over the past two decades have fundamentally transformed the way states conceive their national defence. The Black Sea region, once peripheral in the strategies of great powers, has today become an epicentre of geopolitical tensions. The war in Ukraine, which began in 2014 and escalated dramatically in February 2022, has shifted the parameters of regional security and highlighted the importance of strategic infrastructure for national resilience (NATO, 2021).

In this context, the Danube, with its 1,075 km course through Romanian territory, emerges as a key element in the defensive architecture. The river represents not only a source of resources and a communication route but also a natural barrier with a deterrence role, a highly valuable logistics corridor, and a symbol of Romania's strategic identity.

The concept of *strategic resilience*, developed within NATO and adapted in national strategic documents, implies a state's ability to resist and adapt to major shocks while maintaining the functionality of vital institutions and social cohesion (EACR, 2022). Applied to the Danube region, this concept acquires a particular dimension, where geography, economy, and military security intertwine inseparably.

THE DANUBE – ROMANIA'S GEOSTRATEGIC AXIS

Historical and Military Context

Throughout history, the Danube has witnessed decisive confrontations. In Antiquity, it was the limes of the Roman Empire, the boundary separating the province of Moesia from the "barbarian" territories. In the Middle Ages, it became both a vital trade route and a space of confrontation between the Ottoman, Habsburg, and local powers. During the War of Independence in 1877-1878, the crossing of the Danube by Romanian troops held major strategic and symbolic significance (Giurescu, 2007).

In the 20th century, during both World Wars, the river served as a logistical corridor for the transport of troops, weapons, and supplies. During the Cold War, the Danube was an important element in the Warsaw Pact's defence system but also a bridge to the West.

Goeconomic and Infrastructural Dimension

Today, the Danube is integrated into the Pan-European Transport Corridor VII, connecting the port of Constanța with the Central- and Western-European river and rail networks. The ports of Galați, Brăila, Tulcea, and Giurgiu are multimodal hubs that allow for the rapid transfer of goods between river, rail, and road transport (European Commission, 2020). This infrastructure serves dual purposes: civil and military, making it a major strategic asset.

Relevance to NATO and the EU

Romania's strategic position on the eastern flank of the North Atlantic Alliance, combined with its direct access to the Danube and the Black Sea, gives it an essential logistical role in collective security and defence efforts. This geostrategic position not only ensures the ability to respond quickly to regional threats, but also contributes to the stability and interoperability of the Alliance in the Black Sea region and the Danube basin.

The military mobility on the Danube is a key element in the adaptive defence strategies, being integrated in the crisis preparedness and response plans. The Romanian sector of the river and its ports become critical infrastructures for logistics, facilitating the rapid transit of equipment, materials and forces during multinational exercises and operations, as well as supporting emergency response actions.

This capacity for mobilization and logistics is supported by research in the field of logistics engineering and resource management, which highlights the importance of port infrastructure, transport networks and communication technologies to ensure a fast and efficient response. In addition, the use of Romanian ports for transit of equipment and materials underlines their strategic role in strengthening regional resilience and supporting multinational security efforts.

In the context of the European Union, this position provides the opportunity to coordinate and implement common defence, infrastructure development and risk management policies, thereby contributing to strengthening resilience and promoting stability in the region, in a multidimensional and inter-institutional framework.

By concluding, Romania's position on NATO's eastern flank, combined with access to the Danube and the Black Sea, gives it a crucial logistical role in supporting allied forces. Military mobility on the Danube is already part of the collective defence plans, and Romanian ports have been used for the transit of equipment and materials during multinational exercises and operations (M.Ap.N., 2019).

STRATEGIC RESILIENCE IN THE DANUBE REGION

Resilience in the Danube area means more than just resistance to shocks or disturbances. It involves a complex ability to adapt to changes, whether natural or generated by human activities, as well as the ability to respond and recover quickly in the face of these challenges. In this context, resilience includes:

❖ *Adaptability*: the ability of systems and communities to adjust processes, infrastructure and behaviour to new conditions, such as rising water levels, changes in flows or emerging risks. It requires constant monitoring and flexibility in planning, as well as the use of modelling and simulation technologies to anticipate changes.

❖ *Redundance*: the existence of alternative resources and infrastructures so that, in the event of an incident or failure, critical systems can continue to operate without major disruption. For example, diversification of transport routes, strategic resource reserves and redundant communication infrastructure are essential elements for creating a resilient system.

❖ *Quick restoration capability*: ability to restore essential functions and return to a normal state in the shortest possible time after a disruption. It requires effective intervention plans, sufficient resources and optimal coordination between different components of society, including authorities, communities and the private sector.

Scientifically, these components are fundamental in systems resilience theory, which emphasizes that not only shock resistance, but also the ability to learn and adapt, are key to long-term sustainability. In the case of the Danube, this holistic approach provides more robust protection against various risks, such as extreme hydrological events, pollution or geopolitical threats, contributing to the stability and security of the region.

Protecting critical infrastructure is essential: ports, bridges, power plants, communication systems, and railways in the vicinity of the river must be secured against sabotage and cyberattacks (OSCE, 2021). Additionally, modern surveillance systems – coastal radars, patrol drones, underwater sensors – can ensure early detection of threats.

The river serves as a delaying line in the case of a land offensive, giving defensive forces time to organize their response. At the same time, it is a platform for power projection, allowing for the rapid deployment of ships and supporting ground operations in the riverine areas. The Riverine Flotilla has essential missions of patrolling, escorting, and traffic control, integrating into NATO's plans for defending the eastern flank (ISPI, 2023).

HYBRID THREATS TO THE DANUBE REGION

Hybrid threats combine military and non-military actions to undermine the security of a state without formally declaring war. In the case of the Danube, these may take the form of:

- Sabotage of port infrastructure or navigable channels;
- Cyberattacks on river traffic management systems;
- Disinformation campaigns to erode public trust;
- Economic pressures through control of trade routes.

The conflict in Ukraine has shown that river infrastructure is vulnerable to drone attacks, long-range artillery, and special operations. Sabotages of port warehouses and attacks on commercial convoys in the Black Sea region had direct effects on Danube traffic (European Centre of Excellence for Countering Hybrid Threats, 2021). Recent lessons from this conflict highlight the importance of logistical redundancy, interoperability, and rapid mobility of forces. At the same time, climate change and global economic pressures will bring new challenges for the navigability and security of the Danube, necessitating long-term strategic planning.

LEGAL AND INSTITUTIONAL FRAMEWORK FOR WATERWAY SECURITY

The security of the Danube is governed by a complex set of international and national norms. The *Belgrade Convention* (1948) regulates navigation on the Danube, ensuring free access for riparian states. At the EU level, the *EU Strategy for the Danube Region* includes security objectives, infrastructure protection, and economic cooperation.

In Romania, waterway security involves the Ministry of National Defence, the Ministry of Internal Affairs, the Romanian Naval Authority, and other institutions. The coordination of their actions is vital for preventing and managing incidents.

THE ECONOMIC DIMENSION OF STRATEGIC RESILIENCE

The Danube is a major economic artery. River transport is cheaper and more energy-efficient than road or rail transport, making it essential for Romania's exports and imports. Blocking navigation on the river would have severe economic effects: commercial losses, increased transportation costs, and a decrease in industrial competitiveness (INS, 2021).

Thus, waterway security is not only a military issue but also an economic one. Romania's economic resilience is directly dependent on the uninterrupted functioning of the Danube corridor.

REGIONAL AND INTERNATIONAL COOPERATION ON THE DANUBE

Romania cooperates with riparian states through various formats: the *EU Strategy for the Danube Region*, the *Three Seas Initiative*, and bilateral agreements with Bulgaria, Serbia, and Ukraine. In the security domain, partnerships with NATO and the OSCE are essential for information exchange and coordinating responses to threats (MAE, 2020).

Joint exercises, mixed patrols, and regional command centres are practical ways to increase interoperability and strengthen mutual trust.

FROM PLANNING TO ACTION: MEASURES FOR STRENGTHENING RESILIENCE

Strengthening strategic resilience on the Danube involves the implementation of multidisciplinary measures, based on research in the field of security, engineering and risk management. They aim to increase the capacity to adapt and respond quickly to disruptions, including those generated by climate change and geopolitical conflicts, as follows:

- *Modernisation of the River Flotilla* by introducing state-of-the-art multifunctional vessels and technological equipment, integrated with autonomous navigation systems and environmental monitoring sensors, to ensure the speed and efficiency of interventions in crisis or infrastructure degradation situations.
- *Implementation of an integrated river security system* based on advanced sensing technologies, such as risk detection sensors and air surveillance drones, which enable real-time monitoring of hydrological, environmental and security parameters, thus reducing vulnerabilities and facilitating informed decision making.
- *Creation of logistical continuity plans* based on predictive models and risk analysis to ensure the uninterrupted flow of essential resources and services in crisis or disruption of transport routes.
- *Joint training of the armed and civilian forces*, using scenario-based simulations and exercises, to develop coordination and response skills in complex contexts, in line with best practices in the field of emergency management and national security.
- *Education campaigns for the population in riparian areas*, based on research in the field of social behaviour and strategic communication, to increase the resilience of local communities and create a culture of preparedness and adaptation to multiple risks (M.Ap.N., 2022).

These complementary and synergistic measures will help develop an adaptable resilience system that can effectively respond to emerging challenges and protect the strategic resources of the nation.

CONCLUSIONS

The Danube retains its status as Romania's "*blue bastion*", representing much more than a natural resource or a transport route. It is a pillar of strategic identity and a force multiplier in the equation of national and regional security. From its historical role as a natural frontier and communications corridor to its current function as a logistics artery integrated into NATO and EU networks, the river has consistently proven it can decisively influence both military balance and economic resilience.

The analysis confirms that the strategic value of the Danube derives from its dual character – a natural barrier and a mobility axis. In conventional conflict scenarios, the river can delay and channel the adversary's advance, giving time for defence mobilization. In the context of hybrid threats, the Danube becomes critical infrastructure that must be protected from cyberattacks, sabotage, disinformation, and economic pressures. This complexity means that the security of the Danube region is not exclusively a military matter but one where the political, economic, technological, and societal dimensions inevitably intersect.

From the perspective of military theory and art, the Danube represents a special strategic space, constituting a privileged land for the implementation of the concept of integrated defence. In this context, the river fleet, port infrastructure, law enforcement, civil authorities and international partners must operate as a unified and coordinated system, capable of ensuring early detection, prevention and effective countering of any forms of aggression or disturbance. Moreover, the concept of resilience in this framework is not limited to mere resistance to threats, but also includes the ability to quickly restore the functionality of critical infrastructures and systems, and to adapt operational strategies in crisis conditions. This holistic approach, based on interoperability and flexibility, becomes essential to ensure sustainable security in the Danube region, given the complexity and dynamics of contemporary threats, including hybrid and cyber threats.

BIBLIOGRAPHY:

1. E-ARC/Centrul Euro-Atlantic pentru Reziliență/Euro-Atlantic Resilience Centre (2022). *Reziliența strategică – Cadru conceptual*. București: Centrul Euro-Atlantic pentru Reziliență.

2. Comisia Dunării/Danube Commission (2010). *1948 Belgrade Convention – consolidated text*. Budapest: Secretariat of the Danube Commission.
3. European Commission (2020). *TEN-T Core Network Corridors*. Brussels: European Commission, <https://transport.ec.europa.eu>, retrieved on 2 August 2025.
4. European Centre of Excellence for Countering Hybrid Threats (2021), *Hybrid Threats in Critical Waterways*. Helsinki: HybridCoE, <https://www.hybridcoe.fi>, retrieved on 2 August 2025.
5. Giurescu, C.C. (2007). *Istoria românilor*. Bucureşti: Editura All.
6. INS/Institutul Naţional de Statistică/National Institute of Statistics (2021). *Transportul fluvial în România: Analiză economică*. Bucureşti.
7. ISPI (2023). *River Warfare and Strategic Mobility in Ukraine*. Milan: Italian Institute for International Political Studies.
8. MAE/Ministerul Afacerilor Externe/Ministry of Foreign Affairs (2020). *Cooperarea României în cadrul Strategiei UE pentru Regiunea Dunării*. Bucureşti.
9. MApN/Ministerul Apărării Naţionale/Ministry of National Defence (2019). *Doctrina pentru apărarea teritoriului fluvial*. Bucureşti.
10. MApN/Ministerul Apărării Naţionale (2022). *Planul de mobilitate militară pe flancul estic*. Bucureşti.
11. NATO (2021). *Resilience Guidelines*. Brussels: NATO Headquarters, https://www.nato.int/cps/en/natohq/topics_132722.htm, retrieved on 22 June 2025.
12. OSCE (2021). *Critical Infrastructure Protection in the Danube Region*. Viena: OSCE Secretariat, <https://www.osce.org>, retrieved on 22 August 2025.

ARCTIC NAVIGATION ROUTES: PAST, PRESENT AND FUTURE – STRATEGIC, GEOPOLITICAL AND NAVAL IMPLICATIONS OF THE NORTHWEST PASSAGE AND THE NORTHERN SEA ROUTE –

Navy Captain (Ret.) Associate Professor Dr. Romeo BOȘNEAGU

“Mircea cel Bătrân” Naval Academy, Constanța

DOI: 10.55535/RMT.2025.3.27

The retreat of Arctic sea ice has transformed the Northwest Passage (NWP) and the Northern Sea Route (NSR) from historical curiosities into emerging maritime corridors. Although still limited by environmental, infrastructural and legal uncertainties, these routes are gaining increasing geopolitical and military significance. The paper reviews recent statistics on transits, major Arctic ports and military bases, as well as state strategies, placing Arctic shipping routes in the broader context of global security and trade.

The results show that, although Arctic shipping remains marginal compared to the Suez or Panama Canals, its symbolic and strategic value is growing rapidly. Naval operations, sovereignty disputes and competition between major powers are likely to intensify in the region, requiring cooperative governance mechanisms to prevent militarisation and environmental degradation.

Keywords: Northern Sea Route; military infrastructure; deterrence and submarine operations; autonomous underwater vehicles; Arctic naval operations;

INTRODUCTION

The Arctic has long been perceived as a frozen frontier, accessible only through sporadic explorations and temporary expeditions (AMAP, 2017). AMAP's (Arctic Monitoring & Assessment Programme) geographical coverage extends from the polar Arctic to the sub-Arctic areas of Canada, the Kingdom of Denmark (Greenland and the Faroe Islands), Finland, Iceland, Norway, the Russian Federation, Sweden and the United States, including associated marine areas. AMAP has established a circumpolar region as the focus for its assessment activities, which includes both high Arctic and subarctic areas. In the marine environment, the "AMAP area" includes the northern seas extending to 51°10'N (James Bay, Canada). Within this region, 10 "key areas" have been identified for coordinated pollution monitoring studies. Historically, The Northwest Passage/NWP is known as the desire of people to have a navigable route through the ice between the Canadian Arctic Archipelago and the continent, originating in the 16th century under the name of the Anian Strait – a fictitious sea route between the Pacific and Atlantic oceans sought by Spanish explorers. In practice, the NWP consists of multiple straits and channels crossing the Arctic Archipelago, connecting the North Atlantic, via Davis Strait, with the Beaufort and Chukchi Seas and, ultimately, the North Pacific (Byers, 2013) (*Figure 1*).

The NWP is often presented as a potential "revolutionary breakthrough" for trans-Arctic transport between Asia, North America and Europe. However, its navigability remains constrained by seasonal ice variability, shallow straits and a lack of large-scale infrastructure (Scott Polar Research Institute, 2024). Despite these obstacles, climate change has significantly altered the outlook: ice retreat has made both the NWP and NSR more accessible for commercial and military navigation (IPCC, 2023) (*Figure 2*).

From a geopolitical perspective, the United States wants the Northwest Passage to have the status of an international strait, as opposed to Canada's position, which grants it the status of internal waters under Canadian sovereignty, with significant international implications for maritime transport in the Arctic (Huebert, 2019). Similarly, the Northern Sea Route along the Arctic coast of the Russian Federation is considered by Moscow to be a central element of its Arctic strategy, developed through investments in naval and port infrastructure and modern icebreakers (Conley, Rohloff, 2015; ECFR, 2025).

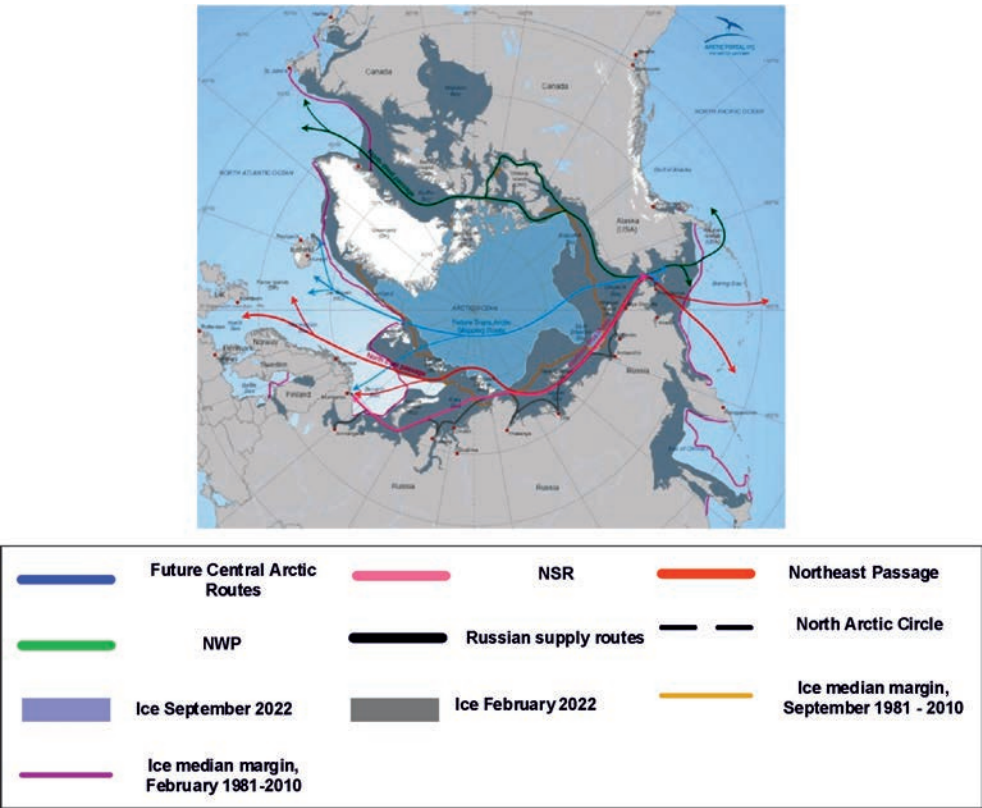


Figure 1: Arctic routes (<https://arcticportal.org/maps>)



Figure 2: Complete transits through the NWP – 2024
(<https://akerarctic.fi/news/international-voyages-on-the-northwest-passage-in-2024/>)

Simulations of various Asia-Europe shipping routes (southern and northern) indicate a significant reduction of over 30% in the distance travelled through the Arctic (Searoutes, 2025; Nouman et al., 2025). However, due to environmental, territorial, geopolitical and military constraints, the adoption of Arctic routes remains problematic. This paper represents a first approach to the past, present and future of Arctic shipping routes, with applications to naval strategy and tactics, military and civilian port infrastructure, and a comparative analysis of their benefits and limitations.

The Northern Sea Route/NSR is considered the shortest sea route between the North-West Pacific and North-West Eurasia, from the Kara Strait, between the Kara and Barents Seas, to Cape Dezhnev, in the Bering Strait. The NSR, approximately 5,600 km long, crosses the Arctic seas: Kara, Laptev, East Siberian and Chukchi, providing access to Russian Arctic ports (Severomorsk, Sabetta, Dudinka, Khatanga, Tiksi and Pevek), as well as ports located along the main Siberian rivers.

Today, supported by Rosatom, an initiative is underway to expand this infrastructure by developing the Northern Sea Route, designed as a strategic maritime transport corridor stretching from Saint Petersburg and Kaliningrad to Vladivostok.

MATERIALS AND METHODS

This research uses a mixed approach, combining historical, empirical and strategic analyses: historical review: Arctic expeditions and naval operations during the Cold War were examined to trace the roots of Arctic geopolitics; Transit statistics: recent data from Rosatom (2025), Aker Arctic (2025) and the Scott Polar Research Institute (2024) were analysed. Policy analysis: the Arctic strategies of Russia, Canada, the United States, NATO and China were evaluated (Government of Canada, 2024; US DoD, 2024); comparative route analysis: distances between Shanghai and Rotterdam were calculated for the Suez Canal, NSR, NWP and Cape of Good Hope routes; geospatial mapping: Arctic ports and military bases were georeferenced.

This integrative approach allows for a balanced understanding of both the commercial opportunities and strategic risks associated with Arctic navigation.

RESULTS AND DISCUSSIONS

Trends in freight traffic

Statistics show that traffic through Arctic routes remains marginal compared to global “mandatory passages” such as the Suez Canal. In 2024, the Suez handled approximately 1.53 billion tonnes of cargo, with traffic of 13,213 ships, while only 37.8 million tonnes were transported through the NSR, with 92 transits recorded (Suez Canal Authority, 2025; Rosatom, 2025; Financial Times, 2025). The NWP recorded only 18 full voyages in 2024, mainly passengers and specialised cargo (Aker Arctic, 2025) (Tables 1, 2, 3 and Figures 3, 4, 5).

Table 1: Freight traffic through Arctic routes versus the Suez Canal (2013-2025), thousand tonnes

Year	Arctic routes	Suez Canal	Sources
2015	n.a.	998,532	Suez Canal Authority (2025)
2016	n.a.	974,184	Suez Canal Authority (2025)
2017	n.a.	1,041,573	Suez Canal Authority (2025)
2018	n.a.	1,139,629	Suez Canal Authority (2025)
2019	n.a.	1,207,085	Suez Canal Authority (2025)
2020	n.a.	1,169,001	Suez Canal Authority (2025)
2021	n.a.	1,274,774	Suez Canal Authority (2025)
2022	n.a.	1,409,879	Suez Canal Authority (2025)
2023	n.a.	1,568,254	Suez Canal Authority (2025) Financial Times (2024)
2024	NSR: 37.8 million tonnes; 92 ship transits NWP: 18 full voyages (passengers/specialised cargo)	1,524,531	Rosatom (2025)
		–	Aker Arctic (2025)
2025	n.a.	238,171 first six months	Suez Canal Authority (2025)

Year	Suez Canal	Year Suez	Suez Canal
2013	n.a.	2020	18,880
2014	n.a.	2021	20,694
2015	17,481	2022	23,851
2016	16,883	2023	26,434
2017	17,550	2024	13,213
2019	18,174	2025	6,055 /first 6 months

Arctic Navigation Routes: Past, Present and Future
 – Strategic, Geopolitical and Naval Implications of the Northwest Passage and the Northern Sea Route –

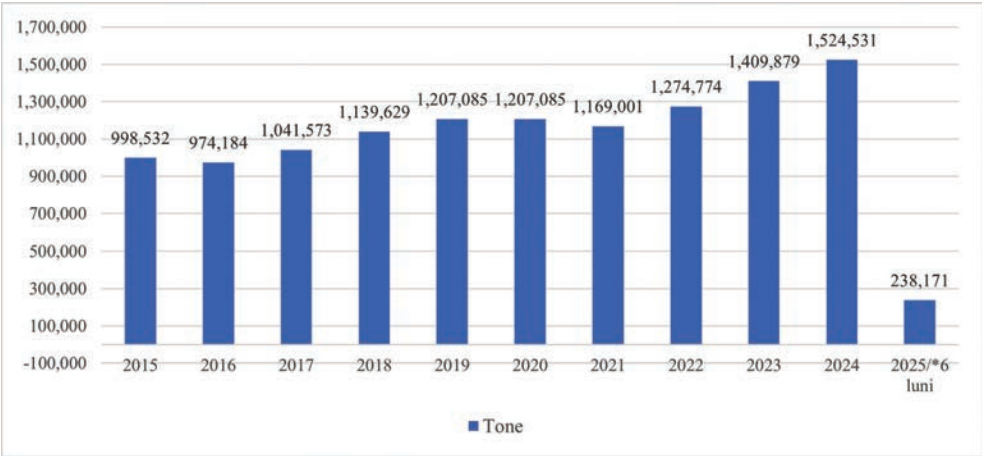


Figure 3: Freight traffic through the Suez Canal, 2015-2025

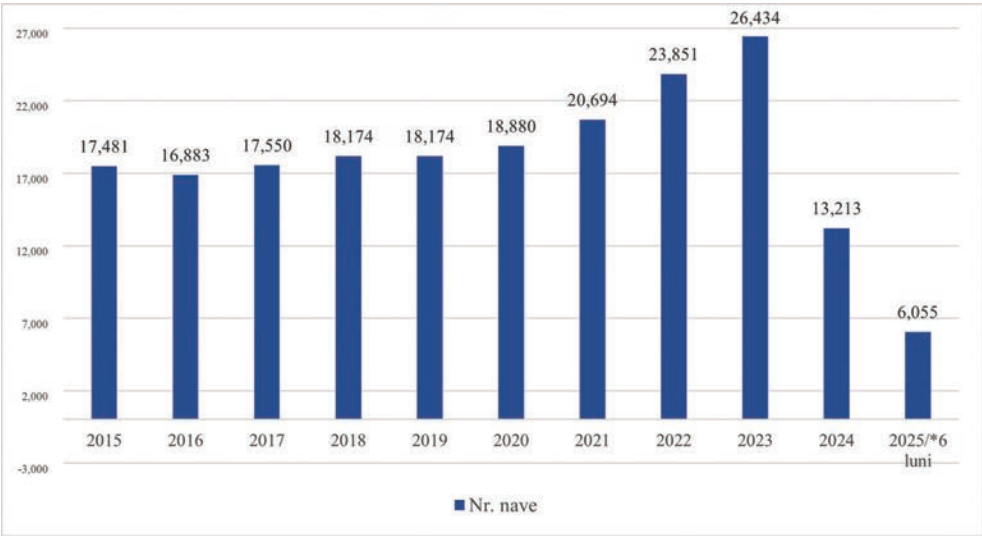


Figure 4: Ship traffic through the Suez Canal

Table 3: Single ship traffic (Arctic Polar Area), 2013-2024

Year	Single ships (Arctic Polar Area)	Year	Unique vessels (Arctic Polar Area)
2013	1,298	2020	1,546
2014	1,370	2021	1,740
2015	1,398	2022	1,677

2016	1,446	2023	1,782
2017	1,446	2024	1,781
2019	1,477	2025	n.a

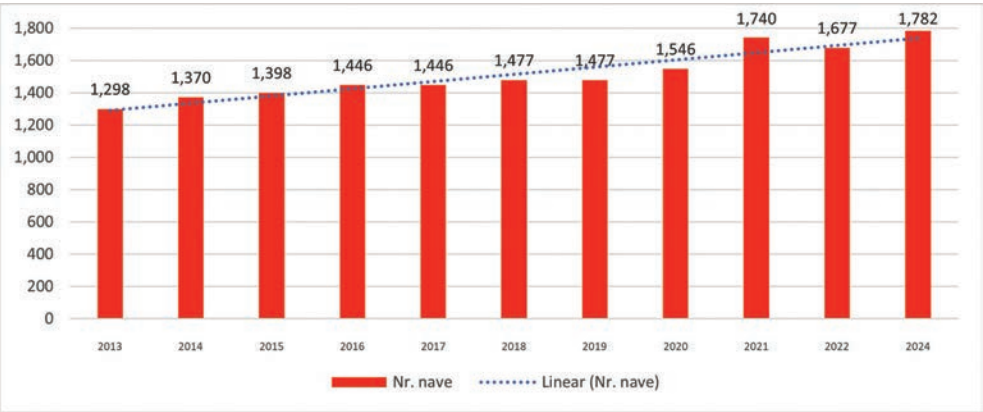


Figure 5: Single vessel traffic (Arctic Polar Area), 2013-2024

These figures confirm that Arctic shipping remains experimental and niche. However, its symbolic and strategic importance far exceeds its commercial contribution.

Distance analysis

The savings in the distance of maritime routes between Asia and Europe are substantial (Table 4, Figures 6 and 7). For example, transport from Shanghai to Rotterdam via the NSR saves approximately 2,050 nautical miles compared to the Suez route, while the NWP offers a similar advantage. However, ice variability and seasonality prevent these routes from functioning as reliable corridors throughout the year (IPCC, 2023).

Table 4: Distances between Shanghai and Rotterdam via different sea routes

Maritime route	Distance (nautical miles)
Suez Suez Canal	10,550
Cape of Good Hope	13,800
NWP	8,700
NSR	8,500

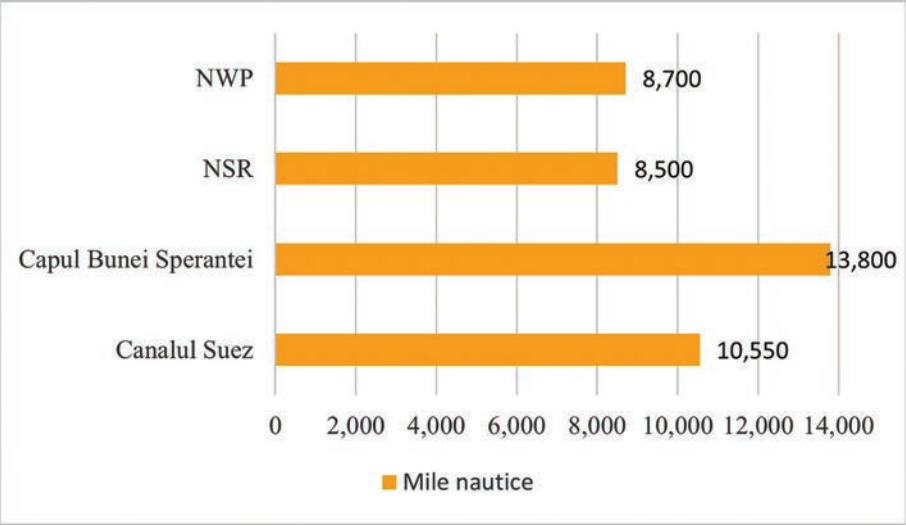


Figure 6: Distances between Shanghai and Rotterdam on different sea routes

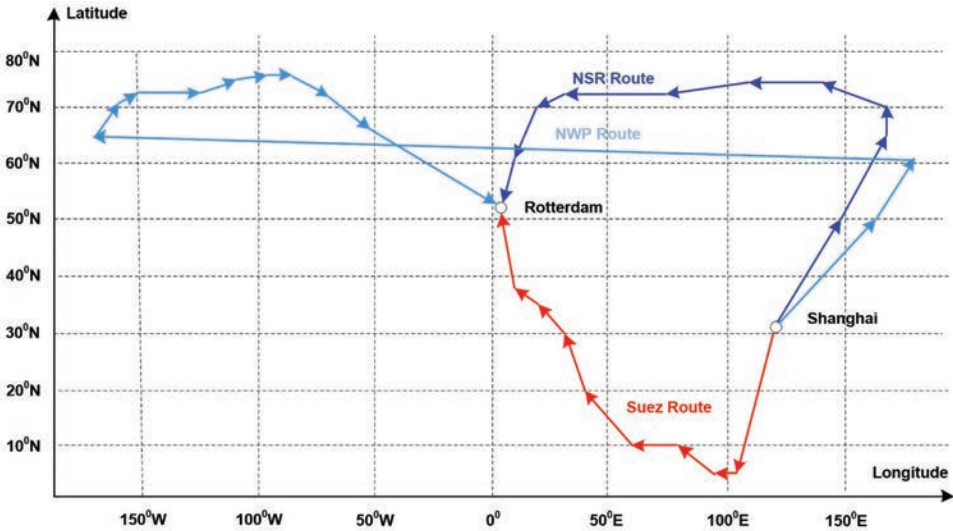


Figure 7: Global shipping routes Shanghai-Rotterdam

Analysis of Arctic port and military infrastructure

The most developed network of civil and military ports is that of the Russian Federation who owns most of the Arctic coastline (53%), where it has built important ports as naval traffic hubs and advanced military bases (Franiok, 2020).

The Russian Federation has 32 permanently monitored military bases in this region. Three of these locations, located in Franz Josef Land, Kotelny Island

and Wrangel Island, can accommodate up to 150 military personnel each (Laws, 2025).

Canada is developing its network of Arctic ports, with the port of Nanisivik currently undergoing modernisation. There are also air bases in the region, such as the American base at Thule (Greenland) and Russian bases. A specific feature of the region is the dual civilian and military use of port infrastructure, which highlights the intertwining of strategic and military interests with the economic interests of the state actors involved here. Thus, the existing infrastructure highlights the dual nature of the Arctic (*Table 5 and Figure 8*). The Russian Federation maintains the most advanced network, centred on Murmansk and Sabetta, complemented by forward military bases such as Nagurskoye.

Table 5: Main Arctic civilian ports and military bases

Port	Country	Port type	Geographical coordinates		
Severnomorsk	Russian Federation	Military	69° 04'N	33° 25'E	
Murmansk	Russian Federation	Civil	68° 97'N	33° 08'E	Ice-free, main hub of the NSR
Sabetta	Russian Federation	Civil	71° 26'N	72° 05'E	
Kirkenes	Norway	Civil	69° 72' N	30° 05'E	logistics
Nuuk	Greenland	Civil	64° 18'N	51° 72'W	Greenland's main port
Nanisivik	Canada	Military	72° 98'N	84° 57'W	Naval base/ planned refuelling
Nagurskoye	Russian Federation	Military	80° 78'N	58° 42'E	Northernmost naval/air base
Thule	Greenland (US/DK)	Military	76° 53'N	68° 70'W	US/Denmark Arctic military base

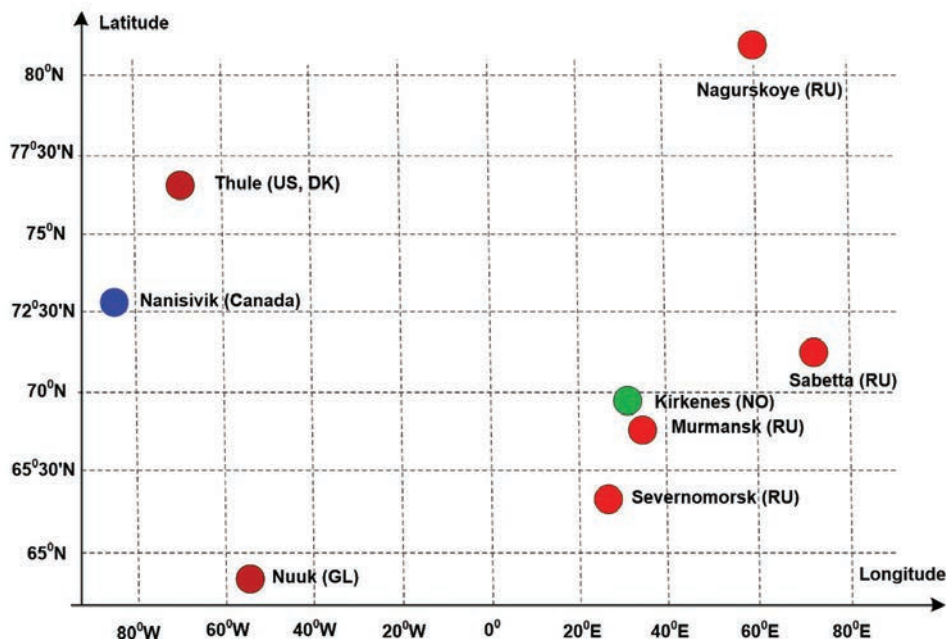


Figure 8: Main Arctic ports and military bases

Future military implications

The Arctic has become the subject of significant economic, military, and geopolitical disputes. Increased use for transportation, exploitation, and the imposition of military force has heightened its strategic importance, which appears to outweigh economic considerations, with implications for regional security. As the ice season shortens due to climate change, the Arctic has become an area of great interest for naval activities, for finding ways to increase freight traffic and, hence, for the development of dual-use (civilian and military) port infrastructure.

Of great importance to the Russian Federation is the modernization of ports and the construction of modern icebreakers to support research and the extractive industry, but also the development of maritime trade by improving military logistics and force mobility.

NATO, China, and other states perceive the Northeast Passage as an area of multi-criteria competition where the changing environment contributes to the intensification of security issues, requiring surveillance, operational research, and realistic terrestrial and maritime environmental forecasts. Thus, this route serves as a case study for the state actors involved here, but also as a new natural laboratory for oceanographic research in support of naval actions, for understanding the situation in the Arctic Ocean, and force projection in contested environments.

Russia seeks Arctic dominance through its fleet of icebreakers, LNG exports, and extensive military infrastructure (Conley, Rohloff, 2015; ECFR, 2025).

Canada emphasises the enforcement of sovereignty over the NWP, supported by Arctic patrol vessels and search and rescue (SAR) capabilities (Huebert, 2019; Government of Canada, 2024).

The United States and NATO prioritise freedom of navigation, deterrence and submarine operations under the ice (US DoD, 2024). China, although located 1,400 km south of the Arctic Circle, declared itself a “*near-Arctic state*” in 2018 and pursues scientific, economic and strategic engagement through the “*Polar Silk Road*” initiative (PRC Arctic Policy, 2018).

Naval operations face unique environmental challenges: extreme cold, unpredictable weather, magnetic anomalies, and limited satellite coverage. Adaptations include: submarine operations under ice, requiring advanced sensors and acoustic mapping; ships with ice-strengthened hulls; icebreakers; autonomous underwater vehicles (AUVs) for reconnaissance and mapping; alternative communications (low-frequency radio, underwater acoustics, experimental fibre optic systems integrated into the ice structure). Arctic naval operations have begun to increasingly integrate multidimensional warfare – at sea, underwater, in the air, and in cyberspace+using hybrid technologies and actions (cyber operations, ecological sabotage, dual-use civilian vessels).

Strategic implications of the Northern Sea Route

The possibility of using this sea route for longer periods of time has transformed it from an internal route to one of international geopolitical and military importance. The extraction of mineral resources, reduced navigation times, and strategic implications are particularly important for military oceanography and maritime security in the region. The Russian Federation has held discussions with both India and China on the route’s potential, with the first meeting of the Russian-Chinese Sub-Commission for Cooperation on the Northern Sea Route taking place in November 2024. This followed a memorandum of understanding between Chinese companies and Rosatom to establish a joint venture for shipbuilding and a year-round container line between Chinese and Russian ports (*Figure 9*).



Figure 9: Russian icebreaker
(<https://world-nuclear-news.org/articles/northern-sea-route-cargo-set-new-record-in-2024>)

Arctic navigation and dual-use infrastructure

Russia's investments in Arctic infrastructure, including port modernization, nuclear-powered icebreakers, and satellite navigation systems, are dual-use in nature. Facilities such as Sabetta and Pevek, while primarily serving energy exports and regional logistics, (Sergunin, 2025). The development of the “Northern Sea Route”, which extends connectivity from Saint Petersburg and Kaliningrad to Vladivostok, enhances Russia's ability to integrate civil and military maritime transport networks, thereby strengthening logistical resilience and force projection capabilities in the Arctic (Staalesen, 2020).

Naval operations and strategic mobility

The NSR offers potential advantages for naval mobility, providing Russia with an “internal maritime highway” connecting its northern and Pacific fleets. This east-west link allows for the rapid redeployment of naval assets, bypassing chokepoints such as the Suez Canal or the Strait of Malacca. At the same time, NATO navies and extra-regional actors such as China view this development with caution, as increased Russian naval access to Arctic waters may alter the regional balance of power (Rahbek-Clemmensen, 2017).

For China, the NSR complements its “Polar Silk Road” strategy, providing alternative sea routes for energy imports and trade security, indirectly strengthening its global maritime presence (Lanteigne, 2019).

Military oceanography and knowledge of the Arctic environment

Marine meteorology and military oceanography will lead to the operationalization of the Northeast Passage. Safe navigation in Arctic waters requires accurate knowledge of sea ice conditions, ocean current patterns, and severe weather phenomena, which are essential for military oceanographic forecasts. Oceanographic buoys, satellites with ice research facilities, and autonomous underwater vehicles are used to study the Arctic marine environment (AMAP, 2021). For war ships, this data is important for safe navigation and for planning surface and submarine naval operations.

Security and environmental dimensions

The increase in shipping traffic along this route raises the level of complexity regarding maritime security. The Russian Federation wants sovereign control over the route in accordance with national legislation, while NATO wants the international principle of freedom of navigation to be respected.

However, shipping traffic here poses environmental risks, resulting in the adaptation of military and civilian operations to minimize the risks of accidents and pollution (Wilson Rowe, 2018).

Oceanographic research and environmental monitoring provide scientific information for the process of strengthening security and sustainability.

Strategic perspective

The broader strategic perspective shows that the Northern Sea Route functions as a trade route and as a strategic area for military oceanography to integrate into global geopolitical competition. The maritime strategy of the future can only be based on top-level oceanographic studies and forecasts, the development of remote sensing, and polar logistics.

The constantly evolving northern Arctic environment will lead to the development of new naval strategies and tactics adapted to the unique conditions of the Arctic region (Wezeman, 2016). In recent decades, climate change and the reduction of the Arctic ice cap have led to a strategic reassessment of the region by the major powers.

The Arctic is becoming an area of influence disputed by the Russian Federation, the United States, Canada, Norway and China, which are stepping up their military and economic presence in the region. Although located 1,400 km south of the Arctic Circle, China declared itself a “*near-Arctic state*” in 2018 and announced plans to become a “*polar power*” by 2030. This goal has been reaffirmed through “*practical cooperation in the Arctic*” and the development of the “*Polar Silk Road*” (Tirziu, 2025).

The new strategies include: advanced deployment of naval forces in Arctic ports such as Murmansk, Severomorsk (Russian Federation) or Dutch Harbor (USA); reactivation of Arctic naval bases, including military airfields; organisation of multinational exercises simulating war scenarios in the Arctic (Williams, 2020).

Military operations in the Arctic require tactics adapted to extreme environmental conditions, with particular challenges: very low temperatures; the presence of sea ice; magnetic anomalies; reduced satellite coverage and unpredictable weather. These conditions have necessitated the adaptation of naval tactics: submarine operations under ice (submarines must be able to navigate under the ice cap and break through the ice to surface). These manoeuvres involve acoustic mapping and advanced sensors; ice-navigating hulls (*Figures 10, 11 and 12*) (Pincus, 2019; Canadian Navy, 2025; Business Insider, 2025); the use of autonomous underwater vehicles (AUVs) and drones for surveillance, reconnaissance, mapping, mine clearance, search and rescue missions, and interactions with isolated communities in the far north; these can operate under the ice cap over long distances, collecting bathymetric data, environmental parameters or sonar images without requiring satellite signals or constant communication links; satellite-free communications (in polar regions, where geostationary satellites cannot be used effectively) – low-frequency radio communications, underwater acoustics or fibre optic communications integrated into the ice structure (experimental) are used for fixed monitoring and real-time data transmission.



Figure 10: Canadian Arctic and offshore patrol vessel – Harry DeWolf class
(<https://www.canada.ca/en/department-national-defence/services/procurement/arctic-offshore-patrol-ships.html>)



Figure 11: Russian Federation Navy ice-class patrol vessel – Ivan Papanin class
(<https://www.bairdmaritime.com/security/naval/naval-ships/vessel-review-ivan-papanin-russian-navy-patrol-ship-with-icebreaking-capability>)

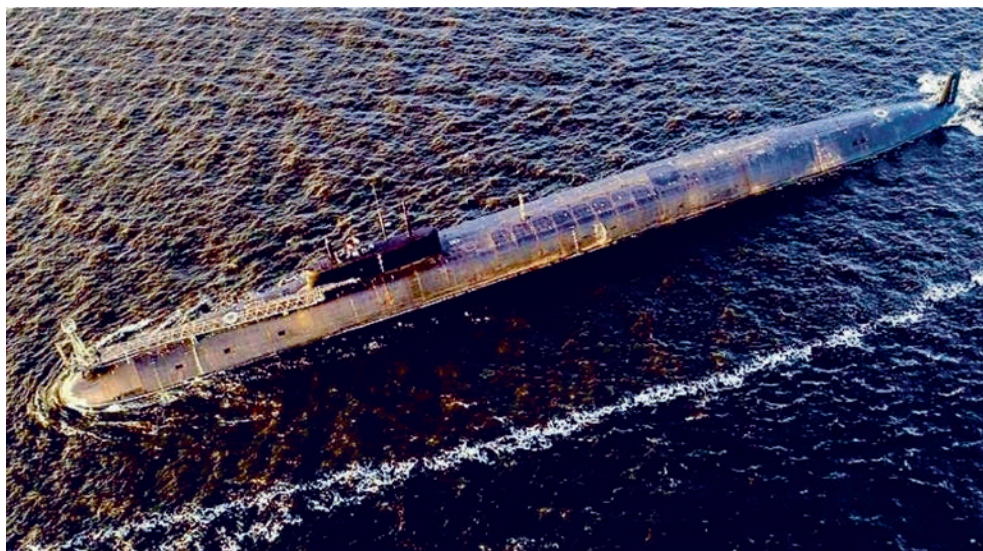


Figure 12: Ballistic missile nuclear submarine, Borei-A class, Russian Federation Navy
(<https://militarywatchmagazine.com/article/160-nukes-russian-navy-boreia-submarine>)

Modern naval doctrines integrate multi-domain operations (maritime, air, cyber and space) in Arctic scenarios. Standardised capabilities and equipment for polar climates are also used in joint exercises. Elements of hybrid warfare are applied (anticipating the use of “grey zone” tactics), through cyber attacks on Arctic infrastructure, ecological sabotage or the use of civilian vessels as cover for military operations.

CONCLUSIONS

Arctic shipping routes are transforming from exploratory routes into geostrategic corridors, although their share in global maritime transport remains negligible.

In my opinion, future naval activities will likely include: sovereignty patrols (Canada, Russian Federation); submarine operations under ice (Russian Federation, United States); escort missions for convoys and LNG carriers (Russian Federation); NATO deterrence exercises and search and rescue (SAR) operations; intensified challenges to transit rights, particularly in the NWP.

In the near future, the Russian Federation has taken steps to modernize and expand the operational capacity of the Northern Sea Route. Rosatom, the state corporation responsible for managing Arctic navigation infrastructure, is taking steps to develop the Russian Northern Sea Route, an extended corridor connecting the ports of St. Petersburg and Kaliningrad in the west with the port of Vladivostok in the east, in order to integrate the NSR into a broader transcontinental transport system. This will be achieved by improving year-round navigability, which will strengthen Russia's position in Arctic maritime logistics and offer an alternative to traditional southern routes, in the context of increasing global shipping traffic and climate change, with major impacts on Arctic sea ice.

China, through its *"Polar Silk Road"* concept, has identified the Arctic as an extension of its *Belt and Road Initiative*, with the aim of securing shorter and more robust supply routes to Europe. Chinese shipping companies have already conducted test voyages along the NSR (with a 22-day voyage for a container ship), demonstrating Beijing's long-term interest in these new maritime trade routes. NATO and Arctic Council states are also closely monitoring developments along the NSR, concerned about the implications for regional security, freedom of navigation, and environmental protection. The gradual retreat of Arctic ice due to climate change is amplifying these dynamics, as longer navigation windows make the route more commercially viable, while also increasing environmental risks.

In this context, the NSR has evolved from a primarily domestic supply route into a corridor of global strategic relevance. Its future trajectory will be shaped by the inter y interaction between technological advances in Arctic navigation, international competition for access and influence, and the environmental constraints inherent in polar ecosystems.

The central challenge lies in balancing the growth of naval presence with cooperative governance mechanisms to ensure navigational safety, SAR coordination, and environmental protection. Without such frameworks, the Arctic risks degenerating into a contested security zone.

BIBLIOGRAPHICAL REFERENCES:

1. Aker Arctic (2025). *International voyages on the Northwest Passage in 2024*. Helsinki: Aker Arctic Technology Inc, <https://akerarctic.fi/news/international-voyages-on-the-northwest-passage-in-2024/>, retrieved on 13 August 2025.
2. AMAP, <https://www.amap.no/about/geographical-coverage>, retrieved on 12 August 2025.
3. AMAP (2017), *Snow, Water, Ice and Permafrost in the Arctic (SWIPA) 2017*. Oslo: Arctic Monitoring and Assessment Programme, <https://www.amap.no/documents/doc/snow-water-ice-and-permafrost-in-the-arctic-swipa-2017/1610>, retrieved on 12 August 2025.
4. Arctic Portal, org. <https://arcticportal.org/maps/download/maps-shipping>, retrieved on 12 August 2025.
5. Byers, M. (2013). *International Law and the Arctic*, Cambridge: Cambridge University Press.
6. Conley, H.A., Rohloff, C. (2015). *The New Ice Curtain: Russia's Strategic Reach to the Arctic*. Washington, D.C.: CSIS, pp. 7-8, <https://www.csis.org/analysis/new-ice-curtain>, retrieved on 11 August 2025.
7. Financial Times (2025). *Shipping lines go cool on Arctic Ocean route*. Financial Times, <https://msiltd.blog/2025/06/09/shipping-lines-go-cool-on-arctic-ocean-route/>, retrieved on 22 August 2025.
8. Franiok, N. (2020). *Russian Arctic Military Bases, American Security Project*, <https://www.americansecurityproject.org/russian-arctic-military-bases/>, retrieved on 22 August 2025.
9. Government of Canada (2024). *Arctic and Northern Policy Framework*. Ottawa: Government of Canada, <https://www.rcaanc-cirnac.gc.ca/eng/1567697304035/1567697319793>, retrieved on 22 August 2025.
10. Huebert, R. (2019). *Cooperation or conflict in the Arctic?*, in *International Journal*, 74(4), pp. 527-545.
11. IPCC (2023). *AR6 Synthesis Report*. Geneva: Intergovernmental Panel on Climate Change, <https://www.ipcc.ch/report/ar6/syr/>, retrieved on 12 August 2025.
12. Komin, M., Hosa, J. (2025). *The bear beneath the ice: Russia's ambitions in the Arctic*. European Council on Foreign Relations, <https://ecfr.eu/publication/the-bear-beneath-the-ice-russias-ambitions-in-the-arctic/>, retrieved on 22 August 2025.
13. Lanteigne, M. (2014). *China's Emerging Arctic Strategies: Economics and Security in the Polar Silk Road*, Institute of International Affairs, The Centre of Arctic Policy Studies, https://ams.overcastcdn.com/documents/Marc_Lanteigne2.pdf, retrieved on 22 August 2025.
14. Laws, J. (2025). *Locations of NATO and Russia's Military Bases in The Arctic Region*, Newsweek, <https://www.newsweek.com/nato-russias-military-bases-arctic-map-2022961>, retrieved on 22 August 2025.
15. Nouman et al. (2025). *Climate Change and Global Sea Routes: Implications for the Arctic and Suez Canal Corridors*, https://www.researchgate.net/publication/395230836_Climate_Change_and_Global_Sea_Routes_Implications_for_the_Arctic_and_Suez_Canal_Corridors, retrieved on 22 August 2025.

16. Pincus, R. (2019). *Three-Way Power Dynamics in the Arctic*, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-14_Issue-1/Pincus.pdf, retrieved on 22 August 2025.
17. PRC (2018). *China's Arctic Policy*. Beijing: State Council Information Office, https://english.www.gov.cn/archive/white_paper/2018/01/26/content_281476026660336.htm, retrieved on 22 August 2025.
18. Rosatom (2025). *Northern Sea Route cargo statistics 2024*, Moscow: State Corporation Rosatom, https://rosatom.ru/en/press-centre/news/new-record-set-for-volume-of-cargo-shipped-along-the-northern-sea-route/?sphrase_id=7031757, retrieved on 22 August 2025.
19. Scott Polar Research Institute, Department of Geography, University of Cambridge, <https://www.spri.cam.ac.uk/>, retrieved on 22 August 2025.
20. Scott Polar Research Institute (2024). *Northwest Passage Transit Records to End of 2024*. Cambridge: University of Cambridge, <https://thenorthwestpassage.info/spri-transits-2020>, retrieved on 12 August 2025.
21. Searoutes (2025). *Route distances: Shanghai–Rotterdam*, <https://www.searoutes.com>, retrieved on 12 August 2025.
22. Sergunin, A. (2025). *Russia's Arctic Strategy. From "Hard" to "Soft" Security*, The Routledge Handbook of Arctic Governance, ed. Elena Conde, Corine Wood-Connelly, <https://www.taylorfrancis.com/books/edit/10.4324/9781003371885/routledge-handbook-arctic-governance-elena-conde-corine-wood-donnelly?refId=6bb251dfe42c-4805-8a5e-151f1ab80e39&context=ubx>, pp. 284-286, retrieved on 22 August 2025.
23. Staalesen, A. (2020). *Russia's new Arctic shipping strategy: boosting traffic on the Northern Sea Route*, The Barents Observer, <https://www.thebarentsobserver.com/arctic/russian-arctic-shipping-could-follow-this-new-route/116282>, retrieved on 22 August 2025.
24. Suez Canal Authority (2025), <https://www.suezcanal.gov.eg/English/Pages/default.aspx>, retrieved on 12 August 2025, accesat la 22 August 2025.
25. Tirziu, A.G. (2025). *China's cultural conquest of the Arctic*, <https://www.gisreportsonline.com/r/china-arctic-culture/>, retrieved on 12 August 2025.
26. US Department of Defence (2024). *Report on Arctic Strategy*. Washington, DC: U.S. Government, <https://www.usa.gov/agencies/u-s-department-of-defense>, retrieved on 12 August 2025.
27. Wezeman, S. (2016). *Military capabilities in the arctic: a new cold war in the high north?*, SIPRI Background Paper, <https://www.sipri.org/publications/2016/sipri-background-papers/military-capabilities-arctic>, retrieved on 12 August 2025.
28. Williams, I. et al. (2020). *America's Arctic Moment: Great Power Competition in the Arctic to 2050*, CSIS, <https://www.csis.org/analysis/americas-arctic-moment-great-power-competition-arctic-2050>, retrieved on 22 August 2025.
29. Wilson Rowe, E. (2018) *Arctic Governance: Power in Cross-Border Cooperation*. Manchester University Press.
30. <https://www.canada.ca/en/navy/corporate/fleet-units/surface/harry-dewolf-class/fact-sheet.html>, retrieved on 22 August 2025.
31. <https://www.com/ukraine-found-weak-points-in-new-russian-nuclear-missile-submarine-2025-8?utm>, retrieved on 22 August 2025.

EMERGING FORMS OF RELIGIOUSLY-MOTIVATED FAR-RIGHT EXTREMISM IN EUROPE AND NORTH AMERICA: RISKS AND PROJECTIONS FOR THE 2025-2030 PERIOD

Dr. Iulian DINULESCU

“Mihai Viteazul” National Intelligence Academy, Bucharest

DOI: 10.55535/RMT.2025.3.28

In recent years, Europe and North America have witnessed the intensification of emerging forms of religiously motivated extremism that diverge from traditional paradigms. This article examines five of the most relevant phenomena in 2025: the Nordic Resistance Movement (neo-pagan racial mysticism), sovereign citizen networks (pseudo-legal religiosity), the “Russian World” ideology (Orthodox-imperial synthesis), QAnon-type conspiratorial syncretisms (apocalyptic Christianity), and Christian Identity/Tradwives currents (biblical fundamentalism and patriarchy). The study employs a comparative approach to highlight their ideological foundations, recruitment mechanisms, transnational networks, and potential trajectories up to 2030. The conclusions emphasize the growing risks these movements pose to democratic institutions, social cohesion, and security, identifying sovereign citizens, QAnon, and the “Russian World” ideology as the most significant impact vectors for the near future.

Keywords: religious extremism; sovereign citizens; Russian World ideology; radicalization; 2030 projections;

INTRODUCTION

Over the past two decades, far-right extremism has become one of the most dynamic and complex challenges to the internal security and democratic order of Western states. Unlike religiously motivated jihadist extremism, which dominated the international security agenda after the September 11, 2001 attacks, recent years have shifted attention toward movements that combine nationalist, racist, and xenophobic ideologies with religious or spiritual references drawn from Christianity, neo-paganism, or conspiratorial syncretisms. This form of far-right extremism, fueled by social and economic crises, political polarization, and recent geopolitical transformations, has gained unprecedented visibility in Europe and North America (Mudde, 2019, pp. 24-48; Ravndal, 2016, pp. 9-10). A distinctive feature of these movements is the use of religion as a source of legitimacy and political mobilization. Whereas in the twentieth century religion was often perceived as a secondary factor within far-right movements, it is now instrumentalized as an integral part of their discourse. Whether through reinterpretations of pre-Christian Nordic traditions, Christian fundamentalist visions promoting “white race” supremacy, or geopolitical constructs that link religion with imperial projects, these movements legitimize themselves by appealing to a “sacralized” past and to a struggle perceived as spiritual against the “enemies of civilization” (Juergensmeyer, 2017, pp. 19-47, 149-181).

Several crises have contributed to the consolidation of these phenomena. First, the 2008 financial crisis and its impact on middle and working classes fueled the anti-system rhetoric of radical right-wing movements (Eatwell, Goodwin, 2018, pp. 180-183). Second, the 2015 migration crisis was instrumentalized to construct narratives of a “foreign invasion” and to justify calls for ethnic and religious purity. Third, the COVID-19 pandemic created opportunities for the proliferation of religiously infused conspiracy theories, particularly in the United States and Germany, where QAnon and affiliated groups integrated apocalyptic Christian elements into anti-vaccine and anti-government discourses (Miller-Idriss, 2020, pp. 45-62). More recently, the war in Ukraine reactivated the “Russian World” ideology, which merges Orthodox religiosity with a neo-imperial geopolitical project. This discourse is dangerous not only for states in Russia’s immediate neighborhood

but also for diasporic communities in Western Europe, where it is propagated through churches and media networks (Suslov, 2024, pp. 234-274).

A critical aspect of religiously motivated far-right extremism is its transnational character. The Nordic Resistance Movement (NRM), for instance, though rooted in Sweden, has established branches in Norway, Finland, and Denmark, while its propaganda circulates freely online (Bjørge, Ravndal, 2020, pp. 37-38). Similarly, the Sovereign Citizens movement, which emerged in the United States, has begun to influence groups in Europe, where its pseudo-religious, anti-state discourse finds fertile ground in contexts of institutional mistrust (Sarteschi, 2020, pp. 1-6, 37, 61). QAnon, initially an American phenomenon, globalized at record speed, and is now present in Germany, France, the United Kingdom, and even Romania, where conspiratorial myths blend with elements of traditional spirituality and religiosity (Argentino, 2025; Dinulescu, 2022, p. 72).

Although far-right extremism is often associated exclusively with secular political ideologies, its religious dimension has become increasingly visible. In the United States, the Christian Identity movement has reinterpreted the Bible to support the idea of white supremacy, while recent currents such as the Tradwives movement employ religious arguments to justify patriarchy and traditional gender roles (Barkun, 1994, pp. 7-8). In Europe, the radical neo-paganism of the NRM sacralizes the struggle for a *“white Europe”* (Dinulescu, 2024-b, pp. 380-381), while the *“Russian World”* ideology merges Orthodox elements with an imperialist political discourse (Dinulescu, 2024-a, p. 68). Religion, therefore, is not merely a discursive ornament but becomes a symbolic and ideological weapon through which these movements construct legitimacy and justify violence. This dimension is essential to understanding why they succeed in mobilizing supporters beyond purely political or economic arguments.

The academic literature on far-right extremism continues to expand. Cas Mudde (2019) and Roger Griffin (2000) have analyzed the ideologies and fascist genealogies of this phenomenon, while Cynthia Miller-Idriss (2020) has studied youth radicalization in the digital age. However, the religious dimension of these movements remains relatively underexplored, even though Mark Juergensmeyer (2017) has demonstrated how religion and violence intersect in multiple contexts. There is thus a clear need to integrate research on far-right radicalism with studies on political religion, in order to better understand how these movements structure their discourse and mobilization.

This article seeks to contribute to this literature through a comparative analysis of the most relevant forms of religiously motivated far-right extremism manifesting in Europe and North America in 2025:

- The Nordic Resistance Movement (NRM);
- The Sovereign Citizens movement;
- The “Russian World” ideology;
- QAnon and conspiratorial syncretisms;
- Christian Identity and the Tradwives currents.

By examining these cases, the article highlights security risks, modes of religious instrumentalization, and possible trajectories through 2030. The analysis goes beyond description to investigate the mechanisms by which these movements become attractive to an increasing number of individuals and the ways in which they manage to transcend national boundaries.

THEORETICAL AND METHODOLOGICAL FRAMEWORK

Defining Religiously Motivated Far-Right Extremism

The study of far-right extremism is a complex field situated at the intersection of political science, sociology, anthropology, and religious studies. In the academic literature, the term “*far right*” is used to describe movements and ideologies characterized by radical nationalism, xenophobia, racism, antisemitism, authoritarianism, and opposition to liberal democratic values (Mudde, 2019, pp. 1-9). In its extremist form, this ideology does not merely express political opinions but promotes violent activism or the systematic subversion of institutions. What distinguishes religiously motivated far-right extremism from other forms is the explicit integration of religion or religious symbols into identity construction and the justification of political action. This religious dimension can take different forms:

- Christian fundamentalism reinterpreted in racist terms (e.g., Christian Identity);
- sacralized neo-paganism (e.g., the Nordic Resistance Movement, which revalorizes Norse mythology);
- Orthodox political religion (e.g., the “*Russian World*” ideology);
- conspiratorial syncretisms with religious accents (e.g., QAnon, which recasts political struggle in apocalyptic terms);
- pseudo-religious legal-conspiratorial frameworks (e.g., sovereign citizens, who invoke biblical quotations or spiritualized interpretations of legal texts).

Mark Juergensmeyer (2017, pp. 25, 202) argues that, in such contexts, religion functions as a *“cosmological scheme”* that transforms social and political conflicts into *“sacred wars”*, where violence is perceived as legitimate and even sanctified. From this perspective, religiously motivated far-right extremism is not merely an expression of political dissent but a form of total mobilization that transcends rational discourse and enters the mythological sphere.

Theoretical Genealogy: Fascism, Nationalism, and Political Religion

Roger Griffin (2000) defines fascism as *“palingenetic ultranationalism”*, that is, an ideology based on the myth of national rebirth following a period of decline. This dimension of *“collective salvation”* is essential for understanding the link between fascism and religion: both promise total regeneration, a return to an *“auroral beginning”*. In this sense, contemporary far-right extremism reprises fascist elements, reinterpreting them in religious terms: the struggle for *“purity”* becomes a sacred mission (Griffin, 2000, pp. xiii, 32, 169, 197). Emilio Gentile (2006, p. 1) conceptualized the notion of *“political religion”*, referring to how totalitarian ideologies use rituals, symbols, and quasi-religious beliefs to mobilize the masses. In the contemporary context, movements such as the *“Russian World”* or the NRM construct a veritable political religion, where Christian or pagan symbols are reinterpreted for political purposes. Robert Bellah (1967) introduced the term *“civil religion”* to describe how modern nations sacralize their institutions and histories. This idea has been extended by Iulian Dinulescu (2024-a), who shows how Russia transforms Orthodoxy into an instrument of imperial ideology. Similarly, Miller-Idriss (2020) notes that in the West, religion is mobilized by radical movements to contest liberal and multicultural hegemony.

The Transnational and Digital Dimension

A central aspect of religiously motivated far-right extremism is transnationalization. While historical fascisms were largely nationalist and localized, contemporary movements employ the internet to construct global networks. Social platforms, online forums, and encrypted applications (such as Telegram) enable the rapid circulation of narratives, transforming local movements into transnational networks (Conway et al., 2019, p. 16). QAnon is the most striking example: from an obscure conspiracy on American forums, it evolved within a few years into a global movement, adopted in Germany as part of the *“Querdenker”* protests and in France as a driver of anti-pandemic restriction demonstrations (Argentino, 2020, pp. 1-12). This adaptability is largely due to its religious dimension: conspiracies are framed as a *“cosmic struggle between good and evil”*,

a universal narrative that transcends national borders. Another example is the Nordic Resistance Movement, which has built a complex online infrastructure including publications, podcasts, and social media channels. Bjørge and Ravndal (2020, p. 40) point out that although the movement limits the use of violence in public actions, it allows for symbolic radicalization in the digital space, where Norse mythology is reinterpreted as an ideological weapon. Thus, one can speak of a digital ecology of religiously motivated far-right extremism, in which myths, symbols, and narratives circulate, combine, and generate new hybrid forms of radicalism.

Research Methodology

The article adopts a comparative approach, analyzing five representative movements:

- The Nordic Resistance Movement – radical neo-paganism and racism.
- Sovereign Citizens – pseudo-legal frameworks with religious and anti-state foundations.
- The “*Russian World*” ideology – Orthodox political religion and imperialism.
- QAnon – apocalyptic conspiracism with religious syncretisms.
- Christian Identity/Tradwives – biblical fundamentalism and patriarchalism.

CASE STUDIES

The Nordic Resistance Movement (NRM)

The Nordic Resistance Movement (Nordiska motståndsrörelsen – NRM) is regarded today as the most influential neo-Nazi organization in Scandinavia and as an emblematic case of how far-right extremism integrates religious and mythological dimensions. Founded in 1997 by Klas Lund, a former militant of the group Vitt Ariskt Motstånd (“*White Aryan Resistance*”), the NRM emerged from the ambition to create not merely a political organization, but a revolutionary movement capable of undermining liberal democracy and establishing a pan-Nordic National Socialist state (Löow, 2015, pp. 38-44). Over nearly three decades, the NRM has expanded its activities from Sweden into Norway, Finland, Denmark, and Iceland, thereby building a transnational network. In Finland, the expansion was strong enough that authorities banned the movement in 2020, with the Supreme Court upholding the verdict on grounds of incitement to hatred and violence (Finnish Supreme Court, 2020). In Norway and Denmark, NRM’s presence is less pronounced but still visible, particularly through marches, public displays, and propaganda campaigns (Bjørge, Ravndal, 2020, p. 38). What differentiates the NRM from other

European neo-Nazi groups is not merely its antisemitic or racist rhetoric – common across this ideological spectrum –, but the way it legitimizes and motivates itself through a constant appeal to Norse mythology. The organization reinterprets runic symbols, mythological figures, and pagan concepts, turning them into a sacralized language of political struggle. The Tyr rune (↑), the arrow associated with the Norse god of war, is used as a central emblem, symbolizing heroic sacrifice and cosmic justice (Gardell, 2003, p. 156). For members and sympathizers of the NRM, political struggle thus becomes an almost religious mission, a confrontation between the pure forces of tradition and the corrupting influences of modernity.

This mythological dimension is not a mere decorative element but functions as a powerful mechanism of radicalization. Mark Gardell (2003, p. 220) emphasizes that the appeal to Norse neopaganism addresses a need for identity and belonging, offering a symbolic framework that turns activism into a spiritual vocation. In this sense, the NRM comes close to what Emilio Gentile (2006, p. 78) described as *“political religion”*, where myths and rituals are instrumentalized to generate loyalty and mobilization. The organization combines street activism – marches in green uniforms, rune banners, posters in public spaces – with a strong online presence. Its websites, podcasts, and social media channels provide not only propaganda but also an alternative culture, including articles, pamphlets, music, and documentaries that consolidate collective identity (Askanius, 2021, p. 148). The Internet thus functions as a genuine *“digital ecology of extremism”* (Conway et al., 2019, p. 5), where symbols and myths are recycled and re-signified, feeding into a globalized collective imaginary. Despite its symbolic appeal, the risks associated with the NRM are tangible. While the leadership officially denies promoting terrorism, cases such as that of Finnish militant Jesse Torniainen – convicted after killing a passerby during a 2016 altercation – demonstrate that individual violence remains a constant reality (YLE, 2018). Europol (2024, p. 38) lists the NRM among groups with a high potential for violence, warning of the possibility that radicalized members might engage in lone-actor attacks.

Looking ahead to 2025–2030, possible scenarios are varied. In a pessimistic scenario, online radicalization could fuel the formation of clandestine cells capable of violent attacks, particularly in the context of geopolitical tensions. A moderate scenario suggests that the NRM will remain numerically marginal but symbolically influential within the transnational far-right network. An optimistic scenario would involve fragmentation and weakening under legal pressure and declining ideological appeal. The most plausible trajectory, however, is the middle-ground scenario: while the NRM is unlikely to become a mass organization, it will continue

to exert cultural and symbolic influence, serving as a radicalization model for other extremist groups in Europe. Its attractiveness lies less in explicit political programs and more in the promise of a heroic, sacralized identity that transforms militants into *“warriors of tradition”*. In conclusion, the NRM illustrates how contemporary far-right extremism merges political ideology with religious mythology, constructing a hybrid vision with long-term radicalization potential. Although numerically small, its symbolic influence and ability to inspire sporadic violence make it a significant actor for understanding the European extremist landscape in the coming decade.

The Sovereign Citizens Movement

The movement known as the Sovereign Citizens Movement represents one of the most complex and difficult-to-classify forms of contemporary extremism. Emerging in the United States in the final decades of the twentieth century, it has evolved from a marginal phenomenon into a diffuse, highly adaptable transnational network with ramifications in Europe and beyond. At its core lies a quasi-religious and mystical conception of law and sovereignty, which reinterprets both the Bible and modern constitutions in ways that challenge the legitimacy of state authority. This fusion of esoteric legalism, conspiracy thinking, and appeals to civil religion makes the Sovereign Citizens a distinctive case within the landscape of right-wing extremism. The roots of the movement can be traced back to the 1970s, particularly to the Posse Comitatus founded by William Potter Gale, which blended elements of Christian Identity with a radical discourse against the U.S. federal government. Gale claimed that ultimate authority in the United States belonged to the *“county sheriff”* and that all other levels of governance – state or federal – were illegitimate. From this ideological base emerged a broader current of opposition to state sovereignty, which gradually developed into what is now called the Sovereign Citizens Movement (Barkun, 2003, p. 95).

During the 1980s and 1990s, fueled by economic crises and disputes over taxation, the movement attracted followers especially in rural states. Its members refused to pay taxes, to acknowledge the legitimacy of courts, or to comply with licensing requirements for driving or business. In 1996, Timothy McVeigh – the perpetrator of the Oklahoma City bombing – was linked by some sources to sovereignist ideology, although he was never a formal member of the movement. This incident placed the movement firmly on the radar of federal authorities (Chermak, Freilich, Simone, 2010, pp. 1019-1041). What makes the Sovereign Citizens academically significant is not only their rejection of authority but also the religious and mystical framework through which they justify their positions. According to Michael Barkun (2003, pp. 2-20), the movement feeds on a mixture

of conspiracy theories, pseudo-legal interpretations, and biblical references, constructing a narrative in which the individual possesses a “divine” sovereignty that precedes the state (Barkun, 1994, p. 5). A central doctrine is the distinction between the “*flesh-and-blood person*” and the “*legal person*” or strawman, a legal fiction allegedly created at birth through the issuance of a birth certificate. In this view, the “real” individual is not bound by state laws, which apply only to the “*fictional*” persona. This doctrine resembles a kind of legal gnosis, whereby initiates discover the “*hidden truth*” and free themselves from state domination (Sarteschi, 2020, pp. 9-29).

At this level, there is a clear overlap with Emilio Gentile’s concept of political religion. The state is demonized and portrayed as a corrupting force, while the individual is presented as the bearer of a God-given sovereignty. Thus, refusing to pay taxes or comply with licensing rules is not merely a political act but almost a sacramental gesture – a reaffirmation of divine freedom (Gentile, 2006, pp. xiv-xv). Some adherents cite biblical passages to justify their defiance of authority, insisting that only “*God’s law*” holds absolute validity, while state legislation represents illegitimate “*usurpation*.” In this way, the Sovereign Citizens situate themselves at the intersection of religion, law, and conspiracy, producing a form of radicalism distinct from other strands of the far right (Gentile, 2006, pp. 23-25). The movement has no centralized hierarchy but functions as a decentralized network. Followers gather in small groups, cells, or act as lone individuals. Their practices vary, but well-known examples include refusal to pay taxes and fines; issuance of fraudulent documents such as “*sovereign passports*” or “*driver’s licenses*”; attempts to establish “*people’s courts*” or “*common law tribunals*”; and confrontations with authorities, sometimes escalating into violence (Dinulescu, 2023-b, pp. 62-66).

In 2010, the FBI classified the movement as a domestic terrorist threat, noting that some of its adherents had carried out armed attacks on law enforcement. For example, in 2010, two police officers were killed in Arkansas by movement members Jerry and Joseph Kane (FBI, 2011). Such incidents demonstrate that, although most sovereign activities are non-violent, the potential for violent radicalization remains significant. While the movement has deep roots in the United States, it has also manifested in fragmented forms in Europe. In Germany, the Reichsbürger (“*Citizens of the Reich*”) phenomenon bears striking similarities to the American Sovereign Citizens. Adherents deny the legitimacy of the Federal Republic of Germany, claiming instead that the Third Reich or earlier state forms still legally exist. Many issue false documents, such as “*Reich passports*” or “*Reich driver’s licenses*”, and refuse to pay taxes. In 2016, a major incident occurred when a

Reichsbürger adherent fatally shot a police officer in Bavaria, confirming the violent risks associated with the movement (Dinulescu, 2023-a, pp. 141, 146; Counter Extremism Project, 2023, p. 9).

Similar groups exist in Austria and Switzerland, inspired by both the German and American models. In the United Kingdom and Ireland, Freeman on the Land currents have gained traction, promoting similar mystical-legal arguments that reject state legitimacy and produce their own documents. France and Nordic countries have reported isolated cases, while in Eastern Europe – including Romania – echoes of the movement appear on conspiracy forums and social media groups, where the idea of “*absolute individual sovereignty*” takes on a spiritual aura and is combined with theories about the New World Order (Dinulescu, 2023-a, p. 139; BfV, 2022, pp. 32-33; Le Sueur, 2011; Europol, 2024; Agache, 2025). Thus, the Sovereign Citizens Movement represents a transnational phenomenon, with local variations united by the same matrix: rejection of the modern state and the sacralization of individual sovereignty. Looking ahead, several scenarios can be envisioned. A pessimistic scenario would involve the transnational consolidation of the ideology, fueled by economic crises and distrust of democratic institutions, with more radical groups potentially shifting from legal nonconformism to organized violence. A moderate scenario suggests that the movement will remain largely marginal yet continue to produce sporadic violent incidents and undermine public institutions. Here, the major risk lies in “*extremist lone wolves*” – radicalized individuals inspired by sovereign doctrine who carry out isolated attacks. An optimistic scenario would involve reducing the appeal of the ideology through a combination of legal, educational, and security measures. However, the past decades show that whenever public institutions experience crises of legitimacy, movements like the Sovereign Citizens tend to re-emerge with renewed strength.

Between 2025 and 2030, it is unlikely that the phenomenon will disappear. Rather, it will adapt to geopolitical and digital contexts. The emergence of hybrid variants, where legal-mystical sovereignism intersects with other forms of far-right extremism or religious conspiracism, appears plausible and worthy of ongoing analysis. The Sovereign Citizens Movement thus exemplifies a form of extremism with religious and conspiratorial foundations that challenges the very basis of the modern state while sacralizing individual freedom. Its American origins have generated a phenomenon that has spread across Europe in various forms, carrying real risks of violent radicalization. Despite its diffuse and decentralized character, the symbolic impact and its capacity to inspire defiance and violence make this movement an actor that requires close monitoring in the coming decade.

The “Russian World” (Russkiy Mir)

When we speak today about the “*Russian World*” – Russkiy Mir – we are not merely referring to a cultural expression. We are dealing with a geopolitical and religious vision that has gradually been transformed from an intellectual discourse into an active instrument of foreign policy and an ideological justification for state objectives. For many observers, Russkiy Mir functions as a bond between imperial nationalism, politicized Orthodoxy, and projects of external influence. In both official and semi-official narratives, the “*Russian World*” includes Russian speakers, adherents of Russian culture, and members of the Russian Orthodox Church — but its elastic nature allows it to be used as a moral argument for political and military interventions in the “*Russophone space*”. Analysts often describe it as the regime’s “*civil religion*” (Laruelle, 2024, pp. 14, 17). The terms and ideas that led to Russkiy Mir emerged in various intellectual circles at the end of the 1980s and throughout the 1990s: philosophers, publicists, and clerics sought to articulate a vision of Russian identity in the face of the Soviet Empire’s collapse. The concept was gradually taken up and “*institutionalized*” – from cultural institutes and foundations (such as the Russkiy Mir Foundation) to the official discourse of the Kremlin and certain church figures. This transition from idea to policy made Russkiy Mir a flexible tool: cultural export in peacetime and ideological justification in times of crisis (Laruelle, 2015, pp. 5-9).

Marlène Laruelle and other scholars have stressed that although Russkiy Mir might appear in public discourse as similar to notions such as Francophonie in its cultural intent, in reality it contains revisionist elements that predispose it to revanchist geopolitical interpretations when placed in the hands of authoritarian actors. In practice, the “*Russian World*” is not a single fixed set of ideas – it operates as a “*geopolitical imaginary*” that can shift from being an instrument of soft power to serving as justification for coercive actions (Laruelle, 2024, pp. 9, 21-22). A defining element of Russkiy Mir is its close connection to the Russian Orthodox Church (ROC). Patriarch Kirill and certain clerical segments have contributed to the sacralization of geopolitical discourse, transforming certain formulations of foreign policy into spiritual terms – even labeling conflicts as “*holy missions*” or “*the protection of the brethren in faith*”. Recent documents and conventions of ecclesiastical bodies have employed language framing war and the “*defense*” of the Russian cultural space in sacred terms, thereby changing the nature of legitimized violence: it ceases to be merely strategic and acquires eschatological meaning for its adherents (Kilp, Pankhurst, 2025, p. 1). This “*sanctification*” of political action has practical consequences: it legitimizes actions that would otherwise appear strictly

geopolitical (annexations, interventions, support for pro-Russian movements) through appeals to the protection of “*Russian communities*” and “*traditional values*”. Recent studies show how discourses within the WRPC (World Russian People’s Council) and other bodies have incorporated religious elements into the moral justification of conflict (Kilp, Pankhurst, pp. 1-8).

Russkiy Mir has been promoted through an organizational mix: cultural foundations, educational programs, media networks, church funding in the diaspora, and “*civic*” NGOs. These elements function as an infrastructure of soft power. State-funded or state-inspired foundations and institutes distribute grants, textbooks, Russian language programs, and cultural projects that build identity ties among diasporas. In parallel, pro-Kremlin media channels and disinformation ecosystems amplify messages whenever political impact is required. Thus, Russkiy Mir acquires not only rhetorical but also institutional and logistical coverage (Laruelle, 2015, pp. 5-9). These instruments serve a dual purpose: in “*normal*” times they operate as cultural bridges, while in times of tension they may be used to generate “*local support*” or provide normative justifications within targeted communities. The annexation of Crimea (2014) and, even more so, the large-scale attack and invasion of 2022 fully illustrated Russkiy Mir’s potential to become a justificatory tool for aggression. Contemporary analyses have shown that Kremlin rhetoric and pro-state actors deliberately employed the concept to “*naturalize*” interventions: Russophone populations would – in the discourse – be “*protected*”

by the motherland, and intervention would be an act of restoring a shared civilizational space. This rhetoric was echoed and amplified by church networks and pro-Kremlin media, providing a moral framework for actions that would otherwise have been framed solely as military operations (Meienberger, 2023, pp. 15, 19).

Scholars such as Anton Shekhovtsov have situated the “*Russian World*” within the broader analysis of how Russian ideology is used to construct historical and geopolitical justifications for revisionism. He demonstrates how cultural narratives can degenerate into political directives with tangible effects on the ground (Shekhovtsov, 2014). In Ukraine, discourses about “*Russian brothers*” or “*civilizational protectorates*” have been used to justify operations to “*protect*” Russophone populations – ranging from “*referendums*” to military actions. In the Baltic states and other countries with Russian-speaking minorities, propaganda based on the “*Russian World*” attempted to exploit either real or fabricated grievances in order to undermine trust in local governments and foster enclaves of loyalty. In many cases, these efforts involved influence infrastructures (media, NGOs, friendly clergy) that prepared the ground for more aggressive actions

when necessary. Comparative studies conducted in recent years document this practice across multiple countries in Eastern Europe and the post-Soviet space (Orzechowski, 2024, pp. 21-25).

Another effect of the Russkiy Mir ideology is its (sometimes opportunistic) connection with segments of the European far right. Recent research shows that certain nationalist groups in Western Europe – attracted by conservative discourse or “*traditional values*” – have engaged in contacts and exchanges with pro-Russian activists, either for ideological collaboration or to develop pro-family, anti-LGBTI, or anti-globalization cultural-political agendas. This alchemy between “*traditionalist*” conservatism and Russkiy Mir rhetoric has created bridges exploitable by influence networks. The 2024 ICCT report maps the ways in which Russian ideas and organizations have built such connections in at least ten European countries (Rekawek et al., 2024, pp. 8-10). The impact of Russkiy Mir on populations has several dimensions:

- Identity: undermining the processes of building a distinct civic identity in host states by appealing to rival ethno-linguistic identities;
- Political: weakening trust in institutions through the promotion of discourses of “*belonging*” to a transnational community;
- Security: directly justifying military or paramilitary actions in the name of protecting the “*Russian World*”.

In short, Russkiy Mir transforms social and cultural vulnerabilities into “*entry points*” for aggressive foreign policy, and through the sacralization of political objectives grants supporters a moral sense for actions that would otherwise appear illegal or immoral (Laruelle, 2024, pp. 23-25). The response to the danger posed by Russkiy Mir must be multi-layered: security countermeasures (monitoring influence networks and countering disinformation), cultural policies (supporting local languages and cultures inclusively), religious dialogue (drawing clear boundaries between independent confessional institutions and state policies), and legal measures when activity enters the illegal sphere (financing interventions, supporting paramilitary groups, etc.). Recent experiences demonstrate that only a combination of measures – not a single one – can limit both the ideological hard power and the cultural soft power (Laruelle, 2015, pp. 14-15).

Ultimately, Russkiy Mir is an idea with multiple forms: cultural, religious, geopolitical. What makes it dangerous is not its ambiguity, but its ability to be used as a political instrument – to create moral legitimacies for interventions, to sacralize conflicts, and to build transnational networks capable of undermining sovereignty and cohesion of states. In the post-2014 and post-2022 world, Russkiy Mir

is no longer merely academic theory: it has become political practice, and in order to understand and counter it, one must analyze it simultaneously from theological, cultural, media, and strategic perspectives (Laruelle, 2024, pp. 5-7, 22, 31).

QAnon and Conspiratorial Syncretisms

The QAnon movement represents one of the most bizarre and at the same time dangerous expressions of contemporary extremism, having a structure that blends digital conspiracism, political messianism, and elements of religious syncretism. Born in the United States in 2017, it quickly spread beyond the Atlantic, finding fertile echoes in Europe, where it intersected with local religious traditions, conspiratorial narratives, and right-wing populism. The QAnon phenomenon represents one of the most visible contemporary expressions of conspiratorial syncretism with a religious foundation, which has managed to transform disparate fragments of narratives, symbols, and doctrines into an almost theological system of interpreting reality (Rothschild, 2021, pp. 12-13). Born in the American digital space but rapidly expanding transnationally, QAnon has become a form of “*conspiratorial religion*” that combines elements of apocalyptic Christianity, Gnostic traditions, and New Age influences, offering adherents a sense of community and cosmic mission (Wessinger, 2021).

The QAnon movement has its origins in the fall of 2017, when a person or anonymous group known under the pseudonym “Q” began posting cryptic messages on forums such as 4chan and later 8kun (Rothschild, 2021, pp. 5-7). The first messages attributed to “Q”, the so-called Q-drops, appeared on the 4chan forum in October 2017, and later migrated to the 8kun platform, as shown in an AFP analysis (Larson, 2021). At its core, QAnon proposes a Manichean narrative in which a single person is described as the providential leader of a cosmic battle between good and evil, while the “*global elite*” – frequently associated with Democrats, progressives, the media, and Hollywood stars – is identified with a satanic cult. The theory was initially regarded as a grotesque fiction, yet its attraction proved contagious. A journalist cited by the Financial Times remarked that an anonymous figure called “Q” presented through cryptic messages the idea of a global conspiracy involving political leaders and other perceived opponents, thereby contributing to the consolidation of conspiratorial narratives in the digital space (Financial Times, 2023). Such narratives not only impose an ordered meaning on social chaos, but also create a sense of participation in an essential struggle, turning followers into a community of “*initiates*” of hidden truth. A central component of QAnon is the blending of religious elements with conspiratorial imagery. From the beginning, “Q’s” messages used apocalyptic language, referring

to an imminent event, The Storm, which was to purify America and restore divine order. This structure resembles millenarian prophecies from the Christian tradition, where believers await a final revelation and judgment of the wicked. As Jason Springs notes, the fascination with conspiratorial theories within evangelical Christian nationalism in the Trump era should not be interpreted as an isolated phenomenon, but rather as a contemporary expression of evangelicals' historical concern with apocalyptic prophecies and the end of time, reflecting how religious beliefs can be mobilized in modern political contexts (Springs, 2021).

These messages, known as Q-drops, claimed to be revelations from within the U.S. administration, suggesting that a global cabal of satanic pedophiles controls the world and that a single providential figure is the savior who will defeat these evil forces (Barkun, 2003, p. 65). The cryptic and fragmentary character of the messages invited collective interpretations, which transformed following QAnon into a permanent hermeneutical exercise (Amarasingam, Argentino, 2020, pp. 37-38). This hermeneutics of secrecy recalls Gnostic traditions, in which truth is hidden and can be revealed only to initiates who know how to "*see beyond appearances*" (Wessinger, 2021). The process of interpreting Q-drops created a participatory framework, similar to a religious community reading and debating sacred texts (Amarasingam, Argentino, p. 38). Thus, QAnon did not stop at producing a conspiracy theory, but generated a mechanism of social and spiritual cohesion, in which meaning arises through the collaboration of believers (Beyer, Herrberg, 2023, p. 2; Dinulescu, 2021, pp. 118-119). Although it did not begin as an explicitly religious movement, QAnon quickly absorbed elements from the American evangelical Christian imaginary, particularly the apocalyptic one (Wessinger, 2021). The narrative of a cosmic struggle between good and evil, of a Messiah who will save the people, and of a final judgment – The Storm – reproduces fundamental themes of Christian eschatology (Rothschild, 2021, p. 5). In parallel, QAnon integrates New Age influences, such as the idea of a "*Great Awakening*", associated both with individual spiritual awakening and with the collective revelation of cosmic truth (Teitelbaum, 2020, pp. 38-51).

This combination led to what Catherine Wessinger described as an "*apocalyptic conspiratorial religion*", in which biblical language and New Age symbols coexist and reinforce each other (Wessinger, 2021). Thus, QAnon manages to attract both evangelical believers concerned with the signs of the end times and followers of alternative spirituality seeking hidden meanings in universal dynamics (Beyer, Herrberg, 2023, p. 6). Participation in QAnon does not involve traditional rituals but rather collective interpretative practices (Amarasingam, Argentino, p. 42). Reading,

analyzing, and discussing Q-drops became forms of “*digital liturgy*”, in which adherents play the role of priestly interpreters (Rothschild, 2021, pp. 97, 222). Instead of physical churches, QAnon communities are organized on social networks, where each group functions as a “*digital parish*” gathering believers around charismatic leaders or influencers (Luban, 2021, p. 9). These online communities provide what sociologists of religion define as “*religious social capital*”: solidarity, recognition, belonging, and existential meaning (Barkun, 2003, pp. 65, 106). They reinforce the feeling that adherents are part of a spiritual and moral elite, capable of seeing the hidden truth ignored by the rest of the world (Wessinger, ib.). One of the most distinctive aspects of QAnon is the centrality attributed to a messianic leader (Rothschild, 2021, p. 69). In the vision of followers, this leader is not merely a politician but the messianic figure chosen by God to fight against the demonic cabal (Barkun, 2003, p. 10). This personification of apocalyptic messianism reinterprets the political leader as a cosmic savior, which explains the almost religious fidelity of followers (Wessinger, 2021). The Storm, the event expected by the community, is described as a final judgment, in which all enemies will be arrested and punished, and world order will be restored (Amarasingam, Argentino, pp. 37, 41). This vision has strong biblical resonances, evoking both the Book of Revelation and Protestant millenarian traditions (Beyer, Herrberg, 2023, pp. 9, 13).

Although it originated in the United States, QAnon quickly spread to Europe and other regions. In Germany, the movement was adopted by Reichsbürger segments and anti-vaccine groups, becoming a catalyst of protests during the COVID-19 pandemic. In France and Italy, QAnon theories merged with anti-globalization discourses and with suspicion toward European institutions (European Commission, 2021, pp. 13, 5). In Eastern Europe, including Romania, QAnon found fertile ground through its intersection with traditional religious discourses about the struggle between good and evil. Thus, conspiratorial ideas were integrated into Orthodox narratives and anti-Western rhetoric, which amplified polarization and mistrust in democratic institutions (Gherghina, Mişcoiu, 2022, pp. 226-227). According to an FBI report, QAnon has been identified as a potential source of domestic terrorist threat, due to the predisposition of some adherents to violent acts (FBI, 2021, p. 1). The events of January 6, 2021, when QAnon supporters participated in the attack on the Capitol, demonstrated that the apocalyptic structure of the movement can mobilize to real violence (Rothschild, 2021, pp. xi-xiii, 27, 46, 72, 89). The mythological structure of the narrative – in which adversaries are demonized as satanic pedophiles – morally justifies any act against them, transforming violence into a form of “*salvation through purification*” (Wessinger, ib.). In this sense,

QAnon falls within the tradition of apocalyptic sects that have generated violence in the name of supreme good (Barkun, 2003, pp. 2-3, 150).

Perspectives 2025-2030. Looking ahead, QAnon demonstrates a remarkable capacity for religious and cultural adaptation (Beyer, Herrberg, 2023, pp. 6-8). The failures of its predictions have not weakened the movement but have been reinterpreted as tests of faith, which strengthen group resilience. Digitalization and political polarization will continue to provide fertile ground for the dissemination of QAnon messages (Rothschild, 2021, pp. 174, 189). It is likely that by 2030 QAnon will become increasingly *“localized”*, integrating figures and symbols specific to national contexts while maintaining its fundamental structure as an apocalyptic conspiratorial religion. This flexibility makes it one of the most persistent and dangerous forms of contemporary conspiratorial extremism (Wessinger, 2021). QAnon has evolved from a collection of anonymous messages into a complex digital religious movement, combining biblical myths, New Age ideas, and political conspiracism within a coherent narrative framework (Rothschild, 2021, pp. 183-198). Functioning as an apocalyptic religion, QAnon offers meaning, community, and cosmic mission in a world perceived as chaotic (Amarasingam, Argentino, pp. 38-39). This combination of factors makes QAnon not only a cultural curiosity but a real threat to Western democracies (FBI, 2021, pp. 1-2).

Christian Identity and the Tradwives Movement

Christian Identity

The movement known as Christian Identity has its origins in the theological reinterpretation of the British Israelism current, an ideology that emerged in Great Britain at the end of the 19th century, which claimed that Anglo-Saxons descended from the lost tribes of Israel (Barkun, 1994, pp. 3-9). In the United States, this doctrine was radicalized, transforming into a racist theology asserting that European whites are *“God’s true chosen people”*, while Jews were considered descendants of Satan (Juergensmeyer, 2017, p. 37). Michael Barkun described Christian Identity as *“a religion”* of hate that provides theological and cosmological justification for violence (Barkun, 1994, pp. 84, 94, 103, 171, 242). This hermeneutic of the Bible became the foundation for a dualistic cosmology in which the final battle between God and Satan was to be fought by white believers against a global system perceived as being controlled by Jews and their allies (ADL, 2017). The idea of a *“holy war”* was central, consistently promoted by leaders such as Wesley Swift, a Californian preacher in the 1940s–1950s, considered the ideological architect of the movement (Barkun, p. 49). In Christian Identity theology, the Bible is reinterpreted to justify both anti-Semitism and white supremacy (Juergensmeyer, pp. 31-37).

The Book of Genesis is read allegorically to support the claim that Jews are the direct descendants of Cain, the “*seed of the devil*”, while populations of color are viewed as pre-Adamic beings, soulless (ADL, 2017). This reinterpretation allows the creation of a “*racial metaphysics*”, where biological differences are sacralized and become theological criteria (Barkun, p. 116). Thus, the ideology is not limited to a mere form of social racism but becomes a religious framework that legitimizes exclusion and violence as divine imperatives (Juergensmeyer, pp. 55, 184). Within this logic, any act of violence against the “*racial enemy*” or the “*Jew-controlled government*” is perceived as a sacred offering in the context of an apocalyptic struggle (ADL, 2017).

Since the 1970s, Christian Identity has served as the spiritual bond for paramilitary and terrorist organizations such as Aryan Nations, The Covenant, the Sword, and the Arm of the Lord (CSA), and The Order (Barkun, p. x). Through these groups, the ideology was translated into violent practice. In particular, Aryan Nations functioned as an informal “*church-state*”, where paramilitary training camps were accompanied by Identity-based sermons (ADL, 2017). In the movement’s literature, leaders are presented as prophets of a final battle against the federal government, labeled as “*ZOG*” (Zionist Occupation Government) (Wessinger, ib.). This formulation became one of the most well-known expressions of extremist propaganda, still used today in far-right circles (AJC, 2025; SPLC, 2024). Christian Identity’s history is marked by numerous acts of violence. The Order carried out a series of robberies and assassinations in the 1980s, including the killing of Jewish journalist Alan Berg in 1984, justified as “*divine punishment*” (Barkun, p. 228). Covenant, the Sword, and the Arm of the Lord stockpiled weapons and explosives, preparing for an insurgency against the United States, until it was forcibly dissolved in 1985 (ADL, 2017). Although Timothy McVeigh, the perpetrator of the Oklahoma City bombing (1995), was not an official member of Identity, researchers have shown that he was exposed to the group’s literature and network through his connections with the Patriot movement (Juergensmeyer, pp. 25, 184). Thus, Identity’s influence on domestic extremist violence is indirect but consistent. Juergensmeyer described these acts as “*sacred performances*”, where violence becomes a liturgy through which believers participate in the cosmic battle between good and evil (Juergensmeyer, pp. 202, 210-211). In this sense, terrorism is no longer perceived as crime but as a form of religious devotion.

Although Christian Identity is a U.S.-originating movement, its elements have been imported to Europe through neo-Nazi networks. The Global Project against Hate and Extremism report notes that fragments of Identity theology can be identified in European groups, where they are combined with local elements

of extremism (GPAHE, 2025b). In the United Kingdom, part of the British Israelism movement radicalized, adopting antisemitic accents inspired by American Identity (Wessinger, ib.). In Europe, far-right organizations have integrated Identity elements into their discourses about “*racial purity*” (GPAHE, 2025-a). In Eastern Europe, although direct influence is more limited, Identity-type ideas circulate online, particularly on conspiratorial networks and forums combining radical Orthodox beliefs with antisemitism (SPLC, 2024). This transnational diffusion demonstrates that in the digital age, radical theologies no longer remain captive to the national context but globalize rapidly. Contemporary perspective and risks until 2030. Today, Christian Identity no longer has strong centralized structures but continues to survive through small networks and the circulation of texts and sermons online (ADL, 2017). Barkun warned as early as 1994 that Identity ideology remains a theological engine for white supremacist violence in rural America (Barkun, pp. 213-218). In a polarized political climate, with low trust in state institutions and the proliferation of conspiracy theories, Identity can provide a religious framework that radicalizes isolated individuals or small cells (Juergensmeyer, pp. 279-280). By 2030, the risk does not necessarily lie in the formation of large organizations but in violent actions by “*lone wolves*” inspired by this theology.

The Tradwives Movement

The movement known as Tradwives has its origins in the online environment, particularly on social media platforms such as YouTube, Instagram, and TikTok, where women promote a lifestyle centered on traditional roles of wife and mother (BBC, 2024). The term “*Tradwife*” is an abbreviation of “*traditional wife*”, designating a woman devoted to family, household, and submission to her husband, inspired by a conservative interpretation of Christian values and post-World War II ideals (The Guardian, 2020). This subculture took shape around 2015-2017, alongside the rise of the alt-right in the United States and the resurgence of anti-feminist discourse online (Rascoe, 2024). During the COVID-19 pandemic, the movement gained increased visibility, as messages about returning to family life and home safety resonated with social and cultural anxieties (BBC, 2024). On the surface, Tradwives present themselves as a personal choice, a “*return to authentic femininity*” and a rejection of modern pressures related to career and emancipation (Rascoe, 2024). Yet behind this rhetoric lies an ideology combining Christian fundamentalism with political conservatism, portraying female submission as a biblical virtue and patriarchal order as the natural foundation of society (Illouz, 2019, pp. 32-35).

The BBC noted that the discourse promoted by Tradwife influencers constructs an idealized representation of traditional femininity, centered on domesticity,

household activities, and obedience to the husband, paradoxically presented as a form of empowerment and an alternative to modern feminist values (BBC, 2024). This rhetorical strategy transforms submission into a paradoxical form of “*empowerment*”, suggesting that true freedom lies in renouncing gender equality (The Guardian, 2020). In many cases, Tradwives claim legitimacy from biblical passages prescribing a wife’s submission to her husband, such as Ephesians 5:22-23 (“*Wives, submit yourselves to your own husbands as you do to the Lord. For the husband is the head of the wife as Christ is the head of the Church, his body, of which he is the Savior*”), turning gender roles into religious imperatives (Ford, 2025). This sacralized framework makes the discourse appear harder to contest, as it is associated with divine will. A distinctive feature of the movement is its online aesthetic. Tradwife influencers use vintage images, retro dresses, baking recipes, and idealized home décor to construct a visual narrative of the family “*golden age*” (The Guardian, 2020). This online performativity (“*pharisaism*”) is meant to create a strong contrast with contemporary feminist culture and to suggest an attractive alternative. Case studies reported in the media highlight families promoting a traditional domestic lifestyle, in which the woman assumes the role of wife and mother, giving up a professional career in favor of household and childcare responsibilities, while the man is seen as the primary financial provider and authority in decision-making (The Independent, 2025). In this way, the movement functions as a tool of cultural socialization, attracting young people through aesthetic images and an apparently positive discourse.

Although Tradwives do not explicitly declare themselves extremist, multiple studies have shown that this subculture intersects with the alt-right and far-right movements (Lewis, 2018, p. 28). Social media, particularly TikTok, has significantly contributed to popularizing the Tradwife phenomenon through influencers promoting domestic aesthetics, heightened femininity, and submission to the husband, attracting millions of followers and transforming this model into a transnational cultural trend (The Independent, 2025). This convergence makes Tradwives a “*soft entry point*” into radical ideologies. Even when not directly claiming affiliation with a religious denomination, the Tradwives movement is imbued with a conservative Christian ethos (Illouz, 2019, pp. 6, 32, 42-47, 240). The concept of submission is often justified through “*divine order*”, and motherhood is presented as a sacred vocation. Thus, religion becomes the invisible framework supporting the entire ideology. The foundation of this lifestyle frequently relies on interpretations of Christian texts emphasizing complementary differences between the sexes. Within this framework, female sacrifice and devotion to family are presented as moral virtues and part of a spiritual vocation (The Independent, 2025). In Tradwife

discourse, the man is invested with the role of protector and family leader, while the woman assumes the position of “*helper*” and household manager, presenting this division of roles not as coercion but as a free and authentic choice, perceived as a means of personal fulfillment (The Independent, 2025). Sociologist Eva Illouz argues that “*the return to tradition often becomes a cover for cultural anxieties and resistance to gender equality*” (Illouz, 2019, pp. 73, 147, 224).

Therefore, Tradwives is not merely a lifestyle phenomenon but a form of cultural counter-revolution with a religious foundation. The Tradwife phenomenon is seen both as an expression of freedom of choice and as a risk for reactivating restrictive patriarchal models. Public debate highlights the tension between valuing domestic traditionalism and perceiving it as a potential social and political regression (The Independent, 2025). The recent popularity of Tradwives is correlated with the rise of conservative currents and reactions to contemporary feminism. Thus, the phenomenon fits into a broader trend of revalorizing traditional gender roles, gaining visibility in digital spaces and fueling cultural and ideological polarization (The Independent, 2025). In Eastern Europe, the phenomenon is less visible as an organized subculture, but the ideas circulate in conservative Orthodox and Catholic communities. Discourses on the “*traditional mother*” and “*submissive wife*” are promoted by religious influencers and conservative politicians, often in opposition to feminism (Illouz, 2019, pp. 6, 23). At first glance, Tradwives may appear benign, centered on personal choice and retro aesthetics. Yet the major risk lies in normalizing authoritarian values and preparing the ground for acceptance of extremist ideologies (Lewis, 2019, pp. 28-29). By 2030, Tradwives are expected to become more mainstream, as they offer an easily digestible message and an attractive aesthetic, which can mask connections to the far right (Lewis, 2019, pp. 8, 33; BBC, 2020). In a European context where illiberal governments promote pronatalist and conservative policies, Tradwives may become a cultural vehicle for these political agendas (The Guardian, 2020).

CONCLUSIONS

The present analysis shows that right-wing religious extremism in Europe and North America can no longer be interpreted as a mere ideological drift, but rather as a complex ecology of transnational movements that use religion both as a source of legitimacy and as a mechanism for emotional and cultural mobilization. Unlike historical forms of extremism, contemporary phenomena – from the racial neopaganism of the Nordic Resistance Movement, to the apocalyptic conspiracism of QAnon, or the pseudo-legal religiosity of Sovereign Citizens – draw their strength

from social vulnerabilities and global crises (economic, pandemic, geopolitical) and derive power from their capacity to combine political, spiritual, and digital dimensions. A central element is the transnational role of religion: beliefs and sacralized symbols are no longer anchored within national contexts, but circulate rapidly online, being locally adapted and reinterpreted. This dynamic transforms religious right-wing radicalism into a threat that cannot be addressed solely through national security frameworks, but requires international and interdisciplinary cooperation. Moreover, the convergence between religious fundamentalism and conservative cultural discourses (as exemplified by the Tradwives phenomenon) demonstrates that the danger does not originate solely from violent groups, but also from seemingly “soft” subcultures that can serve as gateways to radicalization. The online aestheticization of traditional gender roles or the sacralization of ideas such as absolute sovereignty provides fertile ground for the gradual normalization of extremism.

In the medium term (2025-2030), three major trends are emerging:

- The persistence and adaptability of these movements in digital environments, regardless of legal countermeasures.
- Structural fragmentation, with a focus on small cells and individual radicalization, alongside the maintenance of a shared global culture.
- Intersection with geopolitics – particularly through the ideology of the “Russian World”, which sacralizes an imperial project and exports radical religious messages to diaspora communities.

In conclusion, right-wing religious extremism should not be seen merely as a collection of organizations, but as a transnational cultural and religious dynamic capable of eroding democratic institutions through a combination of symbolic violence, apocalyptic discourse, and digital mobilization. The challenge for states and societies will be to respond not only with coercive tools, but through strategies of democratic resilience and cultural dialogue, providing alternative sources of meaning and community in the face of the appeal of extremist narratives.

BIBLIOGRAPHY:

1. ADL (2017). Christian Identity, <https://www.adl.org/resources/backgrounders/christian-identity>, retrieved on 20 September 2025.
2. Agache, V.M. (2025). *Riscul Politic – Arma invizibilă a Imperiului Economic. Cum este subminată suveranitatea națiunilor prin rețele globale de putere financiară, interese corporatiste și instrumente de destabilizare politică*, <https://theodosie.ro/2025/05/29/riscul-politic-arma-invizibila-a-imperiului-economic>, retrieved on 6 September 2025.

3. AJC (American Jewish Committee) (2025). *Zionist Occupied Government (ZOG)*, <https://www.ajc.org/translatehate/Zionist-Occupied-Government>, retrieved on 20 September 2025.
4. Argentino, M. (2025). *QAnon – From Conspiracy Theory to New Religious Movement*. 1st Edition. London: Routledge.
5. Amarasingam, A., Argentino, M.A. (2020). *The QAnon Conspiracy Theory: A Security Threat in the Making?*, *CTC Sentinel*, vol. 13, Issue 7.
6. Askanius, T. (2021). “On Frogs, Monkeys, and Execution Memes: Exploring the Humor-Hate Nexus at the Intersection of Neo-Nazi and Alt-Right Movements in Sweden”, *Television & New Media*, Volume 22, Issue 2.
7. Barkun, M. (1994). *Religion and the Racist Right: The Origins of the Christian Identity Movement*. Chapel Hill: University of North Carolina Press.
8. Barkun, M. (2003). *A Culture of Conspiracy: Apocalyptic Visions in Contemporary America*. Berkeley: University of California Press.
9. BBC (2024). *Trad Wives: The influencers selling 1950s house-wife life*, <https://www.bbc.co.uk/programmes/p0jcx2x5>, retrieved on 15 September 2025.
10. Bellah, R. (1967). “Civil Religion in America”, *Daedalus*, Volume 96, Number 1.
11. Bjørge, T., Ravndal, J. A. (2020). “Why the Nordic Resistance Movement Restrains Its Use of Violence.” *Perspectives on Terrorism*, Volume 14, Issue 6, <https://pt.icct.nl/article/why-nordic-resistance-movement-restrains-its-use-violence>, retrieved on 6 September 2025.
12. Beyer, H., Herrberg, N. (2023). *The revelations of Q: Dissemination and resonance of the QAnon conspiracy theory among US Evangelical Christians and the role of the Covid-19 crisis*, *Zeitschrift für Religion, Gesellschaft und Politik*, Volume 7, Issue 1.
13. Bundesamt für Verfassungsschutz (BfV) (2022). *Verfassungsschutzbericht 2021*. Berlin: BfV, https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/verfassungsschutzberichte/2022-06-07-verfassungsschutzbericht-2021.pdf?__blob=publicationFile&v=8, retrieved on 6 September 2025.
14. Chermak, S., Freilich, J.D., Simone, J. (2010). “Surveying American State Police Agencies about Lone Wolves, Far-Right Criminality, and Far-Right and Islamic Jihadist Criminal Collaboration”, *Studies in Conflict & Terrorism*, Volume 33, Issue 11.
15. Conway, M., Scrivens, R., Macnair, L. (2019). “Right-Wing Extremists’ Persistent Online Presence: History and Contemporary Trends”, *International Centre for Counter-Terrorism*, <https://icct.nl/sites/default/files/import/publication/Right-Wing-Extremists-Persistent-Online-Presence.pdf>, retrieved on 5 September 2025.
16. Counter Extremism Project (2023). *Reichsbürger Movement*, <https://www.counterextremism.com/threat/reichsburger-movement/report>, retrieved on 6 September 2025.
17. Dinulescu, I. (2021). “The Interference of the Far-right Ideology QAnon with Christianity”. *Strategic Impact*, Volume 78, Issue 1.
18. Dinulescu, I. (2022). “Motivation of QAnon Conspiracy Theories Appropriation by Christians and the Expansion of the Phenomenon in 2022”. *Strategic Impact*, Volume 83, Issue 2.
19. Dinulescu, I. (2023-a). *The Risks to Germany’s Peace and Security Generated by The Reichsbürger Movement or “Citizens Of The Reich” Based on Political and Religious Convictions*, in *Romanian Military Thinking*, Issue 4/December 2023.

20. Dinulescu, I. (2023-b). *The Risks to Society Generated by "Sovereign Citizens" Based on the Attitude Influenced by Religious Beliefs*, Studia Securitatis. No. 2/December 2023.
21. Dinulescu, I. (2024-a). *Between the Sacred and the Violent: The Russian Imperial Movement and the New Paradigm of Terrorism*, Studia Securitatis. No. 2/December 2024.
22. Dinulescu, I. (2024-b). *The Nordic Resistance Movement as a Threat to European and International Security*, in *Romanian Military Thinking*, Issue 4/December 2024.
23. Eatwell, R., Goodwin, M. (2018). *National Populism: The Revolt against Liberal Democracy*. London: Penguin Books.
24. European Commission (2021). *Conspiracy theories and right-wing extremism – Insights and recommendations for P/CVE*. By Francesco Farinelli, RAN Expert Pool Member. Luxembourg: Publications Office of the European Union, https://home-affairs.ec.europa.eu/system/files/2021-04/ran_conspiracy_theories_and_right-wing_2021_en.pdf, retrieved on 9 September 2025.
25. Europol (2024). *EU Terrorism Situation and Trend Report (TE-SAT)*. The Hague, <https://www.europol.europa.eu/cms/sites/default/files/documents/TE-SAT%202024.pdf>, retrieved on 6 September 2025.
26. FBI (2021). *Adherence to QAnon Conspiracy Theory by Some Domestic Violent Extremists*, Washington, DC, <https://s3.documentcloud.org/documents/20889411/adherence-to-qanon-conspiracy-theory-by-some-domestic-violent-extremists4.pdf>, retrieved on 9 September 2025.
27. FBI (2011). *Sovereign Citizens: A Growing Domestic Threat to Law Enforcement*. U.S. Department of Justice, <https://leb.fbi.gov/articles/featured-articles/sovereign-citizens-a-growing-domestic-threat-to-law-enforcement>, retrieved on 6 September 2025.
28. Financial Times (2023). *A mind-infecting virus: the dark dreams of QAnon*, <https://www.ft.com/content/de905d13-23d4-4f13-a12d-c66cade6c5aa?>, retrieved on 7 September 2025.
29. Finnish Supreme Court (2020). *Case KKO: 2020:74 – Prohibition of the Nordic Resistance Movement*. Helsinki, <https://korkeinoikeus.fi/en/index/ennakkopaatokset/shortsummariesofselectedprecedentsinenglish/2020/kko.html>, retrieved on 6 September 2025, *apud* Equinet European network of equality bodies. (2020) *Finnish Supreme Court bans Nordic neo-Nazi organization*, https://equineteurope.org/finnish-supreme-court-bans-nordic-neo-nazi-organization/?utm_source=chatgpt.com, retrieved on 6 September 2025.
30. Ford, E. (2025). *How the tradwife social media trend is anti-gospel*, <https://www.erinwrites.ca/writing/2024/3/27/how-the-tradwife-lifestyle-is-anti-gospel>, retrieved on 15 September 2025.
31. Gardell, M. (2003). *Gods of the Blood: The Pagan Revival and White Separatism*. Durham: Duke University Press.
32. Gentile, E. (2006). *Politics as Religion*. Princeton: Princeton University Press.
33. Gherghina, S. Mişcoiu, S. (2022). *Faith in a New Party: The Involvement of the Romanian Orthodox Church in the 2020 Election Campaign, Politics, Religion & Ideology*, Volume 23, Issue 2.
34. Griffin, R. (2000). *The Nature of Fascism*. New York & London: Routledge.
35. GPAHE (2025-a). *Ethnic Cleansing Conference in Europe Draws American Speakers, Advocates for a White Europe*, <https://globalextrremism.org/post/ethnic-cleansing-conference/>, retrieved on 18 September 2025.

36. GPAHE (2025-b). *Europe's White Nationalist Identitarian Movement Ramping up Fundraising Efforts*, <https://globalextrémism.org/post/identitarian-movement-ramping-up-fundraising-efforts/>, retrieved on 18 September 2025.
37. Illouz, E. (2019). *The End of Love: A Sociology of Negative Relations*. Oxford University Press.
38. Juergensmeyer, M. (2017). *Terror in the Mind of God: The Global Rise of Religious Violence*. Fourth Edition. Berkeley: University of California Press.
39. Kilp, A. Pankhurst, J.G. (2025). *The Mandate of the World Russian People's Council and the Russian Political Imagination: Scripture, Politics and War*. *Religions*, 2025, Volume 16, Issue 4 (466).
40. Larson, N. (2021). *Swiss sleuths use text analysis to track down the identity of 'Q' behind QAnon*. *Times of Israel*, https://www.timesofisrael.com/swiss-sleuths-use-text-analysis-to-track-down-the-identity-of-q-behind-qanon/?utm_source=chatgpt.com, retrieved on 7 September 2025.
41. Laruelle, M. (2015). *The "Russian World" – Russia's Soft Power and Geopolitical Imagination*. CGI – Center of Global Interests, May 2015, https://www.researchgate.net/profile/Marlene-Laruelle/publication/344222398_The_'Russian_World'_Russia's_Soft_Power_and_Geopolitical_Imagination_Center_for_Global_Interests_Papers_May/links/5f5d7a0aa6fdcc11640ed901/The-Russian-World-Russias-Soft-Power-and-Geopolitical-Imagination-Center-for-Global-Interests-Papers-May.pdf?, retrieved on 7 September 2025.
42. Laruelle, M. (2024). *Russia's Ideological Construction in the Context of the War in Ukraine*. IFRI (Institut français des relations internationales) report, https://www.ifri.org/sites/default/files/migrated_files/documents/atoms/files/ifri_laruelle_russia_ideology_2024.pdf, retrieved on 7 September 2025.
43. Le Sueur, A. (2011). *Crazy constitutionalism*. UK Constitutional Law Association, <https://ukconstitutionallaw.org/2011/07/22/andrew-le-sueur-crazy-constitutionalism>, retrieved on 6 September 2025.
44. Lewis, R. (2019). *Alternative Influence: Broadcasting the Reactionary Right on YouTube*. Data & Society, <https://datasociety.net/library/alternative-influence/>, retrieved on 15 September 2025.
45. Löw, H. (2015). *Nazismen i Sverige 2000-2014*. Stockholm: Ordfront.
46. Luban, D. (2021). *Hannah Arendt Meets QAnon: Conspiracy, Ideology, and the Collapse of Common Sense*, *Georgetown University Law Center*, <https://scholarship.law.georgetown.edu/facpub/2384>, retrieved on 8 September 2025.
47. Meienberger, A. (2023). *The concept of the "Russkiy Mir": History of the Concept and Ukraine*. *Euxeinos*, Volume 13, Issue 35/2023.
48. Miller-Idriss, C. (2020). *Hate in the Homeland: The New Global Far Right*. Princeton: Princeton University Press.
49. Mudde, C. (2019). *The Far Right Today*. Cambridge: Polity Press.
50. Orzechowski, M. (2024). *Russkiy Mir (Russian World): An Exemplification of All-Russian Nationalism. The Strategy of Neo-Imperial Expansionism of the Russian Federation in Regional and Global Dimensions*. *Polish Political Science Yearbook*, Volume 53, Issue 3.

51. Rascoe, A. (2024). *'Trad wives' are trending. What does that say about feminism today?*. NPR, <https://www.npr.org/2024/01/28/1227453741/trad-wives-are-trending-what-does-that-say-about-feminism-today>, retrieved on 15 September 2025.
52. Ravndal, J. A. (2016). *Right-Wing Terrorism and Violence in Western Europe: Introducing the RTV Dataset*. Perspectives on Terrorism, Volume 10, Issue 3, <https://pt.icct.nl/article/right-wing-terrorism-and-violence-western-europe-introducing-rtv-dataset?#>, retrieved on 6 September 2025.
53. Rekawek, K. Renard, K. Molas, B. ed(s) (2024). *Russia and the Far-Right Insights from Ten European Countries*. International Centre for Counter-Terrorism, https://icct.nl/sites/default/files/2024-04/Russia%20and%20the%20Far-Right%20Insights%20from%20Ten%20European%20Countries%20-%20A4%20e-book_0.pdf?, retrieved on 8 September 2025.
54. Rothschild, M. (2021). *The Storm Is Upon Us: How QAnon Became a Movement, Cult, and Conspiracy Theory of Everything*. Brooklyn&London: Melville House.
55. Sarteschi, C. M. (2020). *Sovereign Citizens: A Psychological and Criminological Analysis*. Cham: Springer.
56. Shekhovtsov, A. (2014). *The "Russian World" will destroy Russia*, <https://anton-shekhovtsov.blogspot.com/2014/08/the-russian-world-will-destroy-russia.html?>, retrieved on 7 September 2025.
57. SPLC (2024). *Christian Identity*. <https://www.splcenter.org/fighting-hate/extremist-files/ideology/christian-identity>, retrieved on 20 September 2025.
58. Springs, J. (2021). *QAnon, Conspiracy, and White Evangelical Apocalypse. Contending Modernities*, <https://contendingmodernities.nd.edu/theorizing-modernities/qanon-evangelical-apocalypse/>, retrieved on 7 September 2025.
59. Suslov, M. (2024). *Putinism – Post-Soviet Russian Regime Ideology*. London: Routledge.
60. Teitelbaum, B. (2020). *War for Eternity: Inside Bannon's Far-Right Circle of Global Power Brokers*. Dey Street Books.
61. The Guardian (2020). *Tradwives': the new trend for submissive women has a dark heart and history*, <https://www.theguardian.com/fashion/2020/jan/27/tradwives-new-trend-submissive-women-dark-heart-history>, retrieved on 15 September 2025.
62. The Independent (2025). *Inside the controversial world of the trad-husbands behind the tradwives*, <https://www.the-independent.com/life-style/tradwife-tiktok-trend-lucky-blue-smith-nara-aziza-smith-b2669137.html>, retrieved on 18 September 2025.
63. Wessinger, C. (2021). *"Cult" Is an Inaccurate, Unhelpful and Dangerous Label for Followers of Trump, QAnon, and 1/6"*. *Religion Dispatches*, <https://religiondispatches.org/cult-is-an-inaccurate-unhelpful-and-dangerous-label-for-followers-of-trump-qanon-and-1-6>, retrieved on 10 September 2025.
64. YLE. (2018). *Neo-Nazi aggravated assault convict requests Supreme Court appeal hearing*, <https://yle.fi/a/3-10137432>, retrieved on 6 September 2025.

THE DEFENCE RESOURCES MANAGEMENT IN THE FRAMEWORK OF THE NEW EUROPEAN SECURITY OBJECTIVES

Colonel Associate Professor Dr. Dumitru IANCU

Associate Professor Dr. Anca DINICU

"Nicolae Bălcescu" Land Forces Academy, Sibiu

DOI: 10.55535/RMT.2025.3.29

The present evolution of economic, social, and military phenomena has strained the existence of individual nations and the sustainability of existing alliances, making stability in these domains a challenging objective to attain in the foreseeable future. But whether at the local, regional, or global level, the problem of guaranteeing the resources required for the operation of a security-providing organization continues to be a major concern for all decision-makers. The European Union, confronted with emerging security problems, deemed it essential to realign European military strategies and outlined new courses of action regarding defense resources by the end of the decade. National defense resource management must swiftly respond to emerging opportunities to maintain strong and sustainable military capabilities.

Keywords: geostrategy; resources; management; collective defense; national security;

INTRODUCTION

In the period 2020-2025, the geostrategic landscape of South-Eastern Europe (EEA) was marked by a pronounced transformation, driven by the complex interconditioning between substantial internal vulnerabilities, global geopolitical tensions and shifts in the European Union's policies. The region, which consists of both EU Member States and Western Balkan countries aspiring to accession, has experienced major external influences that have exacerbated existing threats, risks and vulnerabilities. Domestic factors such as democratic decline and endemic corruption also undermine the capacity for internal resilience, jeopardising the implementation of EU initiatives for the region's economic integration. It is obvious that the success of these efforts will overwhelmingly depend on domestic political will and the state's ability to implement the necessary reforms.

Currently, we believe that the following best describe the primary phenomena and traits of regional security in the Balkans:

❖ *Perpetuating relative political instability and frozen conflicts.* Despite a lot of stability efforts, the region still has “frozen conflicts” due to a number of unsolved ethnic and territorial tensions. The relations between Serbia and Kosovo, but also the political situation in Bosnia and Herzegovina, are relevant examples. Delays in solving these issues or the absence of long-term remedies will keep things unsettled and could lead to escalation.

❖ *Sustaining ongoing external actors' influences.* Throughout its history, as well as today, the Balkans have been at the crossroads of geostrategic rivalry between global and regional powers. Through interconditioning and historical, economic and cultural ties, great powers seek to preserve or increase their influence in the region. These influences have the potential to undermine the Euro-Atlantic integration process of the countries in the region and can fuel internal instability by supporting political forces that are opposed the European path.

❖ *Increasing pressures from hybrid threats.* Current operations, such as information warfare, deception and cyberattacks, generate diversified and complex threats, with growing challenges at the level of each country. They aim to disorganize the functioning of societies, erode trust in democratic institutions or polarize and segment public opinion.

❖ *Increasing dangers generated by the “professionalization” of organized crime.* Most of the countries in the Balkan region with exits/borders to the seas (Black Sea, Aegean Sea, Adriatic Sea or Ionian Sea) were the main geographical feature that led to the transformation of the region into a “turntable” for drug, arms or human trafficking. Countries with developing or stabilizing economies are an environment in which cross-border organized crime groups can easily to organize their illegal activities, undermining the rule of law, corrupting institutions of all kinds, and directly endangering the security and prosperity of nations, in the region and beyond.



Figure 1: Map of South-Eastern Europe
(<https://share.google/images/cFNpjNfKBedzkQ1bB>)

❖ *Increasing economic and energy issues:* The majority of the Balkan nations have relatively low levels of economic investments, inadequate modern infrastructure development, and a high reliance on specific energy sources, elements that make the functioning of local markets vulnerable, as well as the economy of the countries as a whole. It has been repeatedly demonstrated that energy security is an important social milestone; if energy transport projects are blocked or implemented slowly, this leads to a greater reliance on specific suppliers and the hazards that go along with it.

❖ *Slowing down the process of EU enlargement in the area.* The process of accession of the Balkan states to the European Union and NATO has had an increasingly slow pace in recent years. Naturally, neither side can be “blamed” for this, but the prolonged postponement of the integration of these countries can create widespread social frustrations, weaken the strength of pro-European structures in the region and open the way for influence from other state or non-state actors.

The security challenges in the Balkan area are characterised as a complex mix of unresolved historical problems, political-economic vulnerabilities and various threats, and require a clear and convergent approach, based both on concrete Euro-Atlantic integration efforts and on the rapid resolution of internal problems, which are essential actions to ensure the long-term stability of the region.

A SYNOPSIS OF THE KEY GEOSTRATEGIC DEVELOPMENTS THAT IMPACT SOUTH-EAST EUROPE BETWEEN 2020 AND 2025

The period 2020-2025 has been characterized by a series of critical moments in international relations, from the unprecedented global disruption of the COVID-19 pandemic, to the emergence of major interstate conflicts or to the rapid technological acceleration. Without a doubt, these events have led to a significant restructuring of local, regional and global relations. Next, we include some of the most significant phenomena that took place in the EEA area, with an impact on security and defence, as well as:

❖ *Russia's invasion of Ukraine (2022).* The war has mainly influenced the supply of energy and derived resources to the countries in the area, causing negative effects on related prices and the overall economic situation in South-Eastern Europe, as many countries in the region are relatively dependent on Russian gas or transit routes for various raw materials. (Chand, Stilwell, 2022). Regional security has been substantially redefined: national defence and border security have become primary targets in domestic politics; NATO has reorganized and reiterated its function and position in the region; hybrid threats and migration have become the main political concerns in local communities' daily-to-day lives.

❖ *EU enlargement in the Western Balkans.* North Macedonia has officially opened EU accession negotiations, but the process itself is challenging due to bilateral disagreements (especially with Bulgaria) over language, history and minority status (Tidey, 2002; Demjanski et al., 2024). It also notes Albania's intention to accelerate the implementation of its reforms in order to conclude

the accession negotiations started in 2020, with priority being investments in military transport/mobility infrastructure as part of a strategic positioning (Semini, 2025). The EU has maintained its “doors open” for the countries in the region to join the community by providing them with a range of projects and programs, but it has not compromised on meeting the accession criteria or on the timetable assumed by the candidates, which has not resulted in less internal unrest – two factors that are primarily impeding this process.

❖ *Reorganizing defence cooperation in the region.* At the beginning of the year, the trilateral agreement on defence cooperation between Albania (NATO member) - Croatia (NATO and EU member) - Kosovo (non-NATO or EU member) was signed, to improve military interoperability, conduct joint exercises and, potentially share defence capabilities. The agreement is seen as a sign of deeper cooperation in this area between smaller states. (Stojanović, 2025). The initiative was also launched to the other states in the region but generated opposition from Serbia, which considers that previous sub-regional accords on armaments and the risk of the emergence of a new military bloc are affected.

❖ *Maintaining tense relations between Kosovo and Serbia.* The EU has sought and been directly involved in finding constructive solutions to the end of the inter-ethnic disputes in Kosovo – the Ohrid Agreement of December 2022 being the most conclusive example – to create a road to toward normalization (Bytyci, 2023). But local peace is still a long way off, as northern Kosovo is the site of frequent clashes between Serbian protesters and peacekeepers, which has even prompted NATO to increase the military presence in the area (Drăghici, 2023). Both the nations in the region and the EU or NATO will be concerned about regional security as a result of these tensions.

❖ *Societies marked by political instabilities, nationalism and bilateral disputes.* Domestic politics in many EEA states are volatile, with frequent protests, with concerns about the rule of law, corruption and some democratic backsliding. A good example is the case of North Macedonia, where there are specific elements of political instability, with zonal and interethnic dissensions with Bulgaria and Greece and which are corroborated by the rise of right-wing nationalism. (Spasovska, 2024). Additionally, in election processes in some countries (e.g. Romania) there has been defamatory rhetoric, persistent inauthentic online behaviour and the media has proven biased, limiting voters’ ability to make an informed decision and affecting public trust. (OSCE Office for Democratic Institutions and Human Rights, 2025).

The rhythmicity and dynamics of geostrategic events directly impacted the distribution and intensity of associated risks, highlighting regional and global interdependencies. Also, each geostrategic event can restructure the risk matrix by introducing new variables, which can alter the balance of power, regional stability or the response capacity of state or international actors.

Table 1: Matrix for assessing the main geostrategic risks for South-Eastern Europe

Risk	Likelihood	Economic impact	Geostrategic implications
Protracted Russia-Ukraine conflict	High	High (increased energy and food costs, additional defense spending)	Risk of increasing the area of the conflict; restructuring of defence policies at EU and NATO level
Escalation of tensions in the South China Sea/ Taiwan	Medium	High (crisis in the semiconductor market, affecting international trade)	Risk of triggering a new conflict; increasing fragmentation/ disruption of supply chains
Disrupting Rare Mineral Supply Chains	Medium	Medium - high (Increased manufacturing costs, bottlenecks in manufacturing flows)	Risk of increased economic protectionism; geoeconomic/ geostrategic coercion
Cyberattacks on critical infrastructures	High	Medium (interruptions of essential services, financial losses)	Risk of increasing the area of manifestation of hybrid attacks; diminishing the lines of demarcation between the civilian and military domains
Political instability manifested mainly in the great powers	Medium	Medium (increase in customs duties, delays in making major decisions)	Risk of policy incoherence; weakening the power of alliances

SAFE - SECURITY ACTION FOR EUROPE, THE EU'S NEW FINANCIAL INSTRUMENT IN THE FIELD OF EUROPEAN DEFENCE

On March 25 this year, the EU published the new White Paper for European Defence – Readiness 2030 (EDR-2030), in relation to the changes in the strategic environment, it is established that Europe develops a sufficient capacity to deter any military threat, as well as to prevent potential military aggression. The new document explicitly states that *“Member States will always retain responsibility for their own troops, from doctrine to deployment, and for defining the needs of their armed forces. In addition, the EU will always act in a way that does not prejudice the specific nature of the security and defence policy of certain Member States and will take into account the security and defence interests of all Member States”*. (European Union, 2025)

The EU pledges to support and coordinate Member States' efforts to fortify the components of the defence industry and the EU's defence capability, even mentioning European contributions to NATO's deterrence and collective defence. In order to establish a clear predictability for this sector in the long run, it seeks to identify and establish the prerequisite for a significant advance allocation of investments in the defence industry. The ultimate objective of this process is to coherently boost production capacities in the European defence industry.



Figure 2: EU actions for 2030 set out in the White Paper for European Defence
(European Union, 2025)

The creation of an EU Defence Readiness Strategy, which outlines an integrated approach to managing possible conflicts or crises, and an EU Internal Security Strategy, which offers a thorough framework for the efficient prevention, detection, and countering of threats to European security, are also anticipated to supplement this programme document.

Building on the gaps already highlighted by Member States in the area of defence capabilities, this White Paper lays out seven priority areas, which are essential for building a robust European defence. The priority areas are as follows:

❖ **“Air and missile defence:** *an integrated, multi-layered air and missile defence that protects against a full spectrum of air threats (cruise missiles, ballistic and hypersonic missiles, aircraft and UAS).*

❖ **Artillery systems:** *advanced fire systems, including modern artillery and long-range missile systems designed to launch precise, long-range attacks against ground targets (deep precision attack).*

❖ **Ammunition and missiles:** *building on the European External Action Service’s ‘Ammunition Plan 2.0’ initiative, strategic stocks of ammunition, missiles and components, together with sufficient defence industrial production capacity to ensure timely replenishment.*

❖ **Drones and anti-drone systems:** *unmanned systems, including air, land, surface and underwater vehicles, which can be remotely controlled or operate autonomously using advanced software and sensors and improve the capabilities that these technologies enable (e.g. situational awareness, surveillance, etc.).*

❖ **Military mobility:** *an EU-wide network of land corridors, airports, seaports, and support elements and services, facilitating the rapid and smooth transport of troops and military equipment within the EU and partner countries.*

❖ **Artificial intelligence (AI), quantum, cyber and electronic warfare:** *defence applications using military AI and quantum computing; advanced EU-wide electronic systems designed to: protect and ensure the unhindered use of the electromagnetic spectrum for land, air, space and naval forces and operations; suppress, disrupt and prevent the use of the electromagnetic spectrum by an adversary; protect the freedom to operate in space and ensure unfettered access to cyber capabilities. Both defensive and offensive cyber capabilities are necessary to ensure protection and freedom of maneuver in cyberspace. A voluntary support scheme for offensive cyber capabilities needs to be developed together with Member States as a credible deterrent mechanism.*

❖ **Strategic factors for the facilitation and protection of critical infrastructure** including, but not limited to, strategic airlift and air-to-air refueling of aircraft, intelligence and surveillance, maritime domain awareness, use and protection of space and other secure communications assets, and military fuel infrastructure.” (European Union, 2025)

Adopted in May 2025, SAFE (Security Action for Europe) is a new EU financial tool that outlines the distribution of funding to Member States for significant and urgent investments in the European defence sector. This programme aims to revitalize the defence readiness and the development of the European defence industry by providing loans of up to €150 billion through capital markets, under attractive financing conditions, leveraging the EU’s positive credit rating. This initiative supports the EU’s objective of attaining strategic autonomy in the field of defence.

The purpose of SAFE:

❖ **“Supporting urgent defence investments:** Enabling swift and meaningful investments to strengthen the defence industry.

❖ **Improving defence readiness:** Funding helps Member States accelerate their defence readiness.

❖ **Promoting the European defence industry:** SAFE encourages innovation and production in the EU defence sector.

❖ **Achieving strategic autonomy:** By strengthening European defence industrial capabilities, SAFE contributes to the EU’s ability to act independently in the field of defence.” (European Commission, 2025)

SAFE will follow the following application algorithm:

- The European Commission will attract funds from the capital markets.
- The funds raised will be offered to EU Member States in the form of loans.
- Loans should be under favorable financing conditions.

Each EU member currently receives an initial allocation of cash (*figure 3*); the real allocation will be determined by a European resolution in January 2026, following the establishment of each state’s own defence investment plan.

In another interpretation, EDR-2030 represents the strategic vision, “*what we need to do*”, and SAFE is the financial and operational tool, “*how do we do it*”.

EDR-2030 is a strategic document, a long-term vision to modernise Member States’ defence capabilities, with a focus on domestic production, interoperability and the reduction of external dependencies. Its fundamental objective is to transform Europe in “*security provider*”, credible and autonomous.



Figure 3: Provisional allocation of amounts provided for in SAFE
(European Commission, 2025)

Through SAFE, the EU implements the EDR-2030 vision in concrete action, directly financing the projects set out as priorities in the Charter: modernization of the defense industry, joint procurement of ammunition and equipment, or development and equipping with new technologies.

With SAFE, EDR-2030 takes a significant step toward a more cohesive and powerful European Union in the area of defence in the current and future geostrategic context.

CONSEQUENCES FOR MANAGING DEFENCE RESOURCES BY 2030

Given the security context described above and the difficulties posed by the SAFE programme's implementation, we believe the following actions should be part of the management of defence resources in the upcoming timeframe:

❖ *Integrated Military Capability Planning.* The next period will be marked by the launch of the new national defense strategic documents: the National Defense Strategy for 2025-2030, the Defense White Paper and the Military Strategy, which will involve a correlation of the common operational requirements, established at NATO and EU level, with national defense objectives. This approach will ensure the establishment of strategic objectives in the field of defence – national and collective, interoperability targets and the level of effectiveness in the use of resources related to this area. Thus, it becomes extremely important to harmonize military procurement schedules with those of European partners, in order to facilitate

the implementation of joint programs and reduce specific costs. Also, another essential step would be to identify and prioritize the provision of critical capabilities in the short and medium term, as they are nominated in EDR-2030, such as air defense, military mobility and joint logistics.

❖ *Streamlining defence procurement by multinational cooperation.* Objectives such as cutting costs, resolving issues with equipment supply and enhancing interoperability across Member States are central to appropriate action in the field of military procurement. Joint and/or standardised procurement through SAFE will provide the participating nations with the benefits of economies of scale or reduced delivery times of the required capacities. Furthermore, this process must be related to the participation, initiated or later, in the projects coordinated by the European Defence Agency (EDA), on the technical and operational cooperation between nations' directions. In order to develop the technological and industrial basis, another approach might be to provide the framework for the formation of transnational industrial consortia with the goal of merging the defence industries for multiple nations.

❖ *Digitization of defence resources management.* Although this process is undoubtedly new, the structures involved in the management of defence capabilities have not developed it uniformly. Automating these processes would allow increasing operational effectiveness, reducing decision/reaction times, as well as optimizing the use of available resources. A solution in this regard can be the implementation of a military ERP (Enterprise Resource Planning) system, which correlates in real time the missions, operational requirements and specific processes for ensuring equipment, stocks and logistical needs. In order to increase the resilience in the field of defence resources and the ability to react quickly in different situations, it is necessary to connect, with the aid of an advanced digital infrastructure, the national "logistics hubs" with other "logistics hubs" of other European countries.

❖ *Reconfiguration of the strategic reserve and increase the capacity for rapid mobilization.* As a rule, the mobilization capacity and the specific strategic reserve involve the design and prior establishment of possible scenarios for the mobilization of the national defense system, the economy, the population and the territory for defense, as well as the constitution of related logistical reserves, such as materials, ammunition and fuel, etc. These plans must enable all forces involved to act effectively and without delay in the event of a conflict, crisis or natural disaster. In the current geostrategic context, the structural elements of the strategic reserves

must be repositioned in the vicinity of the new areas identified as being a risk to national defense and also must be equipped with modern, secure and digitally managed infrastructure, in order to allow rapid access, traceability and rotation of stocks. From the perspective of EDR-2030, the process of improving defence capabilities at European level will also be based on testing logistics capabilities and improving reaction times, in order to identify possible bottlenecks or deficiencies in the supply chain. Through SAFE, flexible production lines can be created for certain categories of resources, buffer stocks of raw materials, practice the ways of using critical infrastructures specific to European collective defense.

❖ *Training and retention of the human resource specialized in defense.* In defense resource management, this action must be a strategic priority, because only a professional human resource can be able to adequately respond to current and future security challenges. In a context marked by accelerated technologization and increased operational complexity, it is essential that military and civilian personnel in the field of defense resource insurance benefit from continuous and specialized training. Centres of excellence in areas such as logistics or procurement management can contribute substantially to the creation of a shared expertise base at European level. The defense industry is a field in which the human resource must be kept for as long as possible, as the technical and technological requirements related to the operational environment will be in a continuous transformation, so they will not be built from scratch and the experience of the personnel who are already involved in the development of certain production processes already used will overwhelmingly matter. Last but not least, it would be beneficial to develop partnerships between defense institutions, academia and industry, in order to integrate cutting-edge knowledge, innovative or from practice, in the training of personnel.

CONCLUSIONS

The challenges of the current geostrategic context are constantly changing, structurally and in terms of volume, diversity or amplitude. Military conflicts, political and economic tensions, social uprisings, the increase in the area of use of AI, although disparate at first glance, are just some of the landmarks that must be analyzed, monitored and treated from the perspective of national security. Thus, defense resource management is not just a technical process or a specific tool, but must be a modern engine in ensuring resilience and strategic credibility in this field. In an increasingly difficult international environment to forecast,

defense resource management must be characterized by the following features: integrated, collaborative, adapted, fluid and efficient in relation to current geostrategic realities.

BIBLIOGRAPHY:

1. Bytyci, F., (2023). *Serbia, Kosovo reach agreement to implement EU-backed deal normalising ties*, <https://www.reuters.com/world/europe/kosovo-serbia-leaders-arrive-eu-backed-talks-deal-normalise-ties-2023-03-18/>, retrieved on 18 September 2025.
2. Chand, I, Stilwell, A., (2022). *Russian Invasion of Ukraine Impedes Post-Pandemic Economic Recovery in Emerging Europe and Central Asia*, <https://www.worldbank.org/en/news/press-release/2022/10/04/russian-invasion-of-ukraine-impedes-post-pandemic-economic-recovery-in-emerging-europe-and-central-asia>, retrieved on 14 September 2025.
3. Comisia Europeană, (2025). *SAFE – Security Action for Europe*, https://defence-industry-space.ec.europa.eu/eu-defence-industry/safe-security-action-europe_en#:~:text=Adopted%20by%20the%20Council%20of,European%20defence%20industry%2C%20with%20a, retrieved on 23 September 2025.
4. Demjanski, A., Ivanovska, B., Jovanović, B., Milenkovska, S., Pollozhani, L.& Jordanova, M.R. (2024). *North Macedonia: A reform agenda on the path to EU integration*, <https://www.atlanticcouncil.org/in-depth-research-reports/report/north-macedonia-a-reform-agenda-on-the-path-to-eu-integration/>, retrieved on 16 September 2025.
5. Drăghici, M., (2023). *FT: NATO va suplimenta efectivele militare de menținere a păcii în Kosovo*, <https://www.mediafax.ro/politic/ft-nato-va-suplimenta-efectivele-militare-de-mentinere-a-pacii-in-kosovo-21911030>, retrieved on 31 August 2025.
6. European Union, (2025). *White Paper for European Defence – Readiness 2030*, https://defence-industry-space.ec.europa.eu/document/download/98add398-b006-4c68-be28-a276688b0890_en?filename=White%20paper%20for%20European%20defence%20%E2%80%93%20Readiness%202030.pdf, retrieved on 22 September 2025.
7. OSCE Office for Democratic Institutions and Human Rights, (2025), *Competitive Romanian presidential run-off, but campaign marred by hostile rhetoric and inauthentic behaviour online, international observers say*, <https://www.osce.org/odihr/elections/590987>, retrieved on 17 September 2025
8. Semini, L. (2025). *EU foreign policy chief urges Albania to sustain reforms on its path to membership*, <https://apnews.com/article/albania-bosnia-eu-membership-kallas-balkans-9460211d3fa84aa4bd19defddb767a9a>, retrieved on 22 September 2025.
9. Spasovska, B. (2024). *North Macedonia's EU accession: challenges, promises and the way forward*, <https://www.eesc.europa.eu/en/news-media/eesc-info/eesc-info-may-2024/articles/118760>, retrieved on 20 September 2025.
10. Stojanović, M. (2025). *What is the aim of the Declaration on military cooperation between Croatia, Albania and Kosovo?*, <https://europeanwesternbalkans.com/>

2025/03/24/what-is-the-aim-of-the-declaration-on-military-cooperation-between-croatia-albania-and-kosovo/, retrieved on 22 September 2025.

11. Tidey, A. (2022). *For North Macedonia, the opening of negotiations is 17 years in the making*, <https://www.euronews.com/my-europe/2022/07/19/historic-moment-eu-opens-accession-negotiations-with-albania-and-north-macedonia>, retrieved on 30 August 2025.

THE IMPACT OF ARTIFICIAL INTELLIGENCE ON SPECIFIC DEFENCE RESOURCES MANAGEMENT PROCESSES

Associate Professor Dr. Gabriel MĂNESCU

Associate Professor Dr. Sebastian Emanuel STAN

*“Nicolae Bălcescu” Land Forces Academy in Sibiu,
Management Department, Faculty of Military Management*

DOI: 10.55535/RMT.2025.3.30

Artificial intelligence (AI) has fundamentally transformed the management of defence resources by revolutionizing information collection, risk analysis, and scenario planning, while simultaneously maximizing the efficiency of human, material, informational, financial, infrastructure, and research-development and innovation resources. Through advanced algorithms, machine learning, and big data analytics, military organizations now benefit from enhanced real-time decision-making, predictive analysis, and adaptive strategic management. This article synthesizes the latest academic debates and empirical research on military AI, highlighting both its transformative potential and the ethical, operational, and security risks it introduces.

Keywords: artificial intelligence; augmented decision-making; cyber security; defence resources; managerial processes;

INTRODUCTION

The new paradigms of defence resource management reflect the necessity of continuous adaptation to technological shifts and the complexity of contemporary threats. As Sarjito (2024) aptly points out, *“AI has become the essential engine of innovation within military structures, enabling a dynamic and coordinated response to emerging risks”*. This perspective is echoed by Mayer (2023, p. 521), who notes that *“AI technologies are shaping new procedures for planning and executing of military operations, involving a profound transformation at tactical and strategic levels”*. The integration of AI requires data convergence, resource interconnectivity, and rapid alignment with global dynamics, amplifying the importance of the managerial process as a vector as strategic performance (Rashid et al., 2023; EPRS, 2025).

THEORETICAL FOUNDATIONS OF AI IN THE DEFENCE

In the context of defence, artificial intelligence (AI) is approached as a multidisciplinary set of theories, algorithmic models, and machine learning paradigms that integrate computer science, elements of advanced statistics, cognitive psychology, and, naturally, engineering disciplines. The classic definition of AI, according to Nilsson (2009), encompasses *“any system capable of functioning intelligently and with foresight in a dynamic environment”*, an aspect also highlighted by Mayer (2023), who differentiates between traditional automated systems and the new generation of autonomous systems *“capable of adaptation, independent decision-making, and recalibration in operational contexts”*.

An essential conceptual pillar lies in the way the two fundamental paradigms of AI development are approached:

- the symbolic (top-down) approach, focused on expert systems and logical rules, suitable for tasks with well-defined rules (Mayer, 2023, p. 522);
- the connectionist (bottom-up) approach, focused on artificial neural networks capable of extracting patterns from massive datasets (Russell, Norvig, 2016).

In recent years, Machine Learning (ML) algorithms – Deep Learning (DL) – have enabled automated object recognition, intelligence document analysis, scenario modelling, anomaly detection, autonomous decision-making, and even strategic risks forecasting (Rashid et al., 2023; Mayer, 2023; Sarjito, 2024). Within the vast

and complex field of defence, these techniques are refined and implemented into audio and video recognition systems (ISR, SIGINT), autonomous platforms (drones, ground vehicles), and decision intelligence software for dynamic analysis of multi-source data, such as *Project Maven*, the *Global Information Dominance Experiment* (GIDE), and many others.

Another fundamental concept, well established in the military field, is the *DIKW* (Data-Information-Knowledge-Wisdom) hierarchy, which illustrates how AI transforms raw data collected from a wide range of sources (sensors, cyber networks, etc.) through pattern recognition and semantic integration into decision-making information and operational knowledge (Russell, Norvig, 2016; Mayer, 2023; Sarjito, 2024). In parallel with this concept, *Signal Detection Theory* explains the important role of AI in rapidly discriminating between relevant signals and informational noise in a complex security environment, supporting agile reactions and strategic foresight (Wickens et al., 2004).

Most often, AI applications are classified according to seven basic models (Rashid et al., ib.):

- autonomous systems.
- goal-driven systems.
- pattern and anomaly recognition.
- predictive analytics.
- assisted decision-making.
- human-machine conversation and interaction.
- hyper personalization/contextual adaptation.

These patterns are present in technologies such as facial recognition, autonomous vehicles, predictive maintenance, AI-assisted logistics management, virtual/ intelligent reality-based training and simulation, self-optimizing sensor networks, and rapid decision-making tools (Mayer, ib.; EPRS, 2025).

Systems Theory (Bertalanffy, 1968), the *Technology Acceptance Model* (TAM) developed by Davis in 1989, and *Complex Adaptive Systems* models govern the adoption and integration of AI into military structures, emphasizing cyber resilience, interconnectivity and the development of fully automated or hybrid OODA (Observe, Orient, Decide, Act) loops that are fully automated, or only hybrid (Mayer, ib.; Sarjito, ib.).

Theoretical and methodological innovation continues in the AI domain, showing trends toward the integration of symbolic and connectionist paradigms (hybrid AI), developing autonomous platforms with meta-learning capabilities, and adapting to the expansion of electronic warfare and modern hybrid operations (Rashid et al.; Mayer, ib.; EPRS, 2025).

TRANSFORMING DEFENCE RESOURCE MANAGEMENT PROCESSES THROUGH AI

Before detailing the impact of AI on each specific defence resource, it is important to recall that the managerial process in the defence domain represents “the set of activities of planning, organizing, coordinating, training, commanding, and controlling-evaluating the efficient use of resources in order to achieve the objectives of the military organization” (Webster et al., 1989; Iancu, 2023; EPRS, 2025). All these processes are vital because they ensure the rapid adaptation of the military system to changes in the strategic environment, maximize the value of available resources, and proactively anticipate risks, aspects that become critical in the context of pressures generated by digitalization and the explosion of AI.

Human Resources

The integration of AI into the management of human resources in the defense sector has generated significant transformations in the efficiency, objectivity, and adaptability of managerial processes. Machine learning algorithms and certain specialized platforms enable the automation of recruitment, selection, training, and evaluation processes, raising operational performance to high standards (EPRS, 2025).

Staff recruitment and selection processes benefit from systems (such as HireVue or Pymetrics) that analyse video interviews and questionnaire responses, identifying the behavioral and professional skills appropriate for the position, which leads to a reduction in subjectivity and an increase in the accuracy of decisions regarding the recruitment and selection of the best candidates (Rashid et al., ib.).

Another particularly important aspect of human resource management is the continuous evaluation of staff performance and the generation of adaptive feedback, achieved through solutions such as Workday, SAP Success Factor, or IBM Watson Talent. These platforms can aggregate data from daily activities, reports, and simulations, enabling the development of personalized professional development plans (Mayer, ib.). A relevant example in this regard is the implementation of the “Sgt. Star” chatbot by the US Army, which uses natural language processing techniques to answer questions about recruitment, training, and careers, demonstrating increased efficiency in communicating with candidates and military personnel.

At the European level, the French and German defence ministries use advanced analytics platforms to forecast staff turnover, plan rotations, and identify “talent” within the organization early on (EPRS, 2025).

Among the advantages of centralising this data with AI is the constant monitoring of physical and psychological health. AI also facilitates the generation of predictive reports on future personnel needs and the identification of risks related to collective and individual performance, providing military decision-makers with that mix of superior tools for strategic decision-making (Mayer, *ib.*; EPRS, 2025).

However, it is imperative to develop a set of ethical regulations to ensure algorithmic transparency, decision-making accountability, and the prevention of discrimination in the military environment (Mayer).

Material Resources

The management of material resources in the defence sector requires an integrated approach to AI as a determining factor for optimizing logistics, procurement, maintenance, and inventory management processes (STS Romania, 2023; Ilie, 2024). The importance of these processes stems from the need to ensure operational continuity, rapid response to requests from the theatre of operations, and increased resilience of military structures in dynamic and unpredictable contexts (Jianu, 2014; Ilie, 2024).

Military inventory tracking and management systems widely use automatic recognition tools and techniques (RFID, IoT sensors) and ERP-type platforms with AI modules, facilitating real-time monitoring of equipment, ammunition, food, and spare parts. In the US, the Defence Logistics Agency (DLA) uses over 55 AI models to forecast requirements, prevent stock shortages, detect counterfeits, and optimize procurement strategies, reducing costs by 15-20% and increasing the reliability of specific operations (Traxtech, 2025).

Predictive maintenance, based on machine learning algorithms and the analysis of patterns in military equipment and technology operating data, allows for the anticipation of failures and the optimization of the maintenance cycle. Furthermore, the use of AI for predictive maintenance extends the life cycle of equipment and technology, reduces repair costs, and increases the availability of military equipment and technology. An example of this is the Datategy platform, which provides examples of predictive analysis for a wide range of engines that power US Army equipment (Datategy, 2025-a; Soules et al., 2022).

In terms of operational logistics, the use of autonomous AI-piloted drones for logistics transport, reconnaissance, and rapid supply in hard-to-reach or high-risk areas is transforming traditional paradigms (Infosys BPM, 2025; Verbitskaya, 2025). Navigation algorithms, obstacle avoidance, load management, and energy optimization allow for timely adaptation to weather conditions, significantly reduce delivery times, and minimize resource consumption (Soules et al., *ib.*).

The most important AI tools used in material resource management and a brief description of them are presented in the following figure.

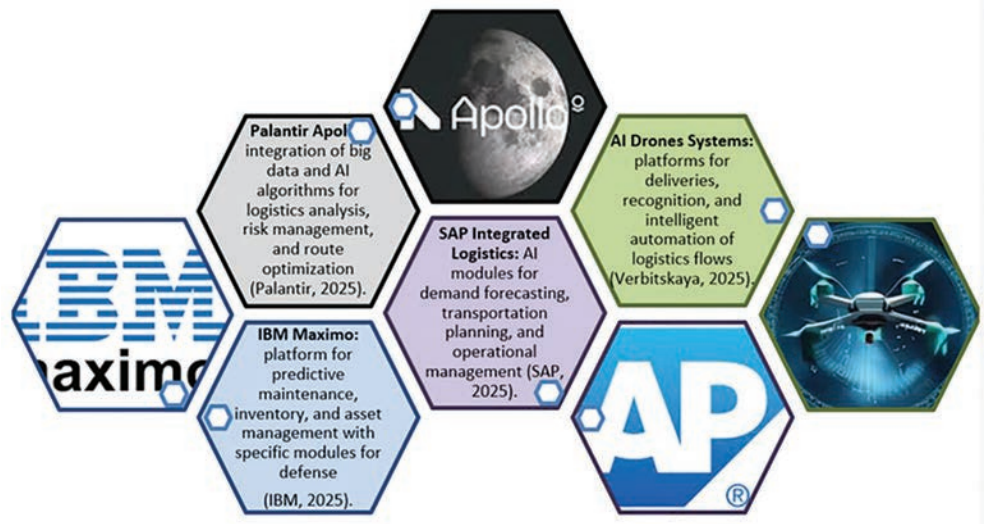


Figure 1: Artificial Intelligence Tools Used in the Management of Material Resources

Through the implementation of these tools, logistics systems become more agile, scalable, and resilient – responding optimally to the demands of the modern military operational environment (Ilie, 2024; STS Romania, 2025; Traxtech, 2025).

Informational Resources

Information resource management in the defence sector has been revolutionized by the application of AI, which provides the mix of information needed by military decision-makers for faster decision-making and advanced protection against cyber threats. Moreover, AI is *“the key element in the transformation of data analysis, surveillance, and cyber intelligence processes”* (Mayer, p. 524).

Big data, pattern recognition, and anomaly detection algorithms enable the rapid synthesis of large volumes of data, identifying potential threats or informational opportunities in near real time, generating integrated and relevant operational dashboards (Rashid et al., 2023; King, 2024; Sarjito, ib.). Furthermore, AI supports early identification and management of information crises, providing rapid decision support (Johnson, 2019), which is also reflected in Mayer’s (2023, p. 526) words regarding the purpose of AI implementation, namely that *“AI fundamentally changes the structure of managerial decision-making, reducing uncertainty and increasing the ability to respond to cyber-attacks and disinformation campaigns”*.

Within NATO, the *Information Environment Assessment* (IEA) uses AI to monitor the global information environment, assessing influence activities, social behaviours, and narrative dissemination patterns, with support for operational and strategic decisions (NATO ACT, 2025). AI-assisted analyses such as Narrative Analysis, Sentiment Analysis, and Social Network Analysis are already widely implemented to identify fake news, disinformation operations, and understand relevant social developments in real time (Maathuis, Cools, 2025).

On the cybersecurity side, platforms such as *Darktrace* and *Microsoft Defender AI* monitor network behaviour, detect anomalies, and react almost instantly to cyberattacks, raising the level of protection and reducing incident response time (Fortinet, 2024; Bonnemaïson, 2025). At the same time, AI algorithms are used for robust assessment of vulnerabilities in military networks, identification of risks such as data poisoning, evasion attacks, or pattern theft. An example of this is the *Securing Artificial Intelligence for Battlefield Effective Robustness* (SABER) project developed by DARPA (2025).

The implementation of these key applications and AI tools in the field of information resource management brings benefits on the one hand, but on the other hand, they come with or generate certain challenges that the military organization must give due importance to. By automating data filtering, aggregation, and synthesis, AI significantly reduces response time, increases the accuracy of analyses, and ensures information superiority, especially in the spectrum of hybrid and cyber conflicts (FlySight, 2023; McKinsey, 2025). However, there are increased risks of attacks on sensitive AI systems, susceptibility to data falsification, or the propagation of algorithmic errors without human supervision (King, 2024; DARPA, 2025).

Financial Resources

AI is bringing about significant changes and transformations in financial resource management, optimizing budgeting, fraud detection, and strategic financial planning processes (EY, 2025), facilitating automatic analysis of budget execution, and quickly detecting fraud or anomalies through transaction analysis (AOSR, 2023; EPRS, 2025). Predictive models help simulate financial scenarios and allocate funds based on anticipated risks (ECA, 2019). According to Sarjito (2024, p. 28), “management processes are thus optimized by reducing expenses and increasing the traceability of financial execution”, with defence sector institutions thus making the transition from reactive models to proactive processes, increasing the efficiency and transparency of financial execution (Zentner, 2025).

Advanced platforms such as *IBM Cognos* and *SAP S/4HANA for Defense* are used for automated budget analysis, financial risk management, and transaction auditing, substantially reducing administrative costs and processing time (EY, 2025; Singh, 2025).

In terms of financial fraud prevention, AI has become indispensable through systems such as *Tookitaki*, *Fortinet*, and *TMForum*, which identify abnormal behaviour patterns in real time and block suspicious transactions (Fortinet, 2024; Tookitaki, 2025). Such networks use neural networks and anomaly detection to combat phishing, embezzlement, and corruption (TMForum, 2023).

In the strategic budget planning segment, the *ThroughPut* and *Artiv AI* platforms enable financial scenario simulation and allocation optimization, accelerating the decision-making process and reducing human error (DefenseOne, 2024; ThroughPut, 2025). Recent analyses highlight a sharp increase in the share of spending on AI and autonomous systems in global military budgets (Markets and Markets, 2025).

Defence Infrastructure

The Russian-Ukrainian conflict has once again highlighted the importance of defence infrastructure. In military terms, defense infrastructure is defined as *“the permanent buildings and facilities necessary to support, deploy, and operate a nation’s armed forces”* (RAND, 2025). The specialized literature in our country uses the concept of territorial infrastructure, which represents *“all the works, objectives, and facilities that, built in peacetime, can be used for defence purposes in crisis situations or at war, in order to amplify the advantages and properties offered by the national geographical factor, in order to maintain the viability and reliability of the national defense system and the entire economic and military potential.”* (Cernăianu, 2006). As can be easily seen, the Romanian interpretation is much more integrative and emphasizes the moment of capitalizing on this type of resource.

AI has a significant impact on the protection and optimization of defence infrastructure, acting on and, at the same time, transforming each component of this resource, with an emphasis on both the logistical and the cybernetic and operational components.

By integrating AI into critical infrastructures, the armed forces gain the ability to quickly detect threats, automate monitoring and maintenance processes, increase operational resilience, and ensure both physical and digital security (Datategy, 2025b; EPRS, 2025).

Advanced AI solutions are implemented for continuous surveillance of military installations, fusion of data from multiple sensors (radar, IR, EO, sonar), early

identification of anomalies, and effective risk management. Platforms such as Scylla AI demonstrate over 96% accuracy in threat detection, and AI-Driven Sensor Fusion combines and interprets data from multiple diverse sensors – such as cameras, LiDAR, radar, and inertial sensors – to produce a more accurate, comprehensive, and intelligent understanding of an environment or system than any individual sensor could achieve. This technology enables smarter decision-making and provides deeper insights, leading to advances in areas such as autonomous vehicles, predictive maintenance in industrial environments, and enhanced situational awareness in defence applications (Aquah, 2025; Shaw, 2024).

For defence infrastructure resilience, AI is used both at the risk management level –simulating attack, sabotage, or failure scenarios – and at the operational management level (Datategy, 2025). Recent studies emphasize that the integration of AI into defence infrastructure is essential for maintaining the operational superiority and responsiveness of military systems in contested and/or complex environments (Shaw, 2024; PwC, 2025).

Research, Development, and Innovation (RDI) Resources

The integration of RDI resources is a fundamental pillar of military modernization, ensuring rapid adaptation to disruptive technologies such as AI, robotics, drones, autonomous systems, and digitization. The substantial investments made in recent years by the Ministry of National Defence in this area aim, in the medium and short term, to develop in-house capabilities for designing, testing, and implementing state-of-the-art technologies, while stimulating collaboration with international partners and innovative companies (Construct Intelligence, 2025; Mihălțianu, 2025).

Projects such as the national drone program, Romanian *MALE UAV* platforms, and partnerships with global technology leaders (Baykar, Elbit Systems, Thales, Shield AI) demonstrate that RDI resources are directed both towards the development of national know-how and the transfer of advanced technology. Companies such as OVES Enterprise and Carfil Braşov are investing heavily in research and development and manufacturing drones for complex missions, while partnerships with international entities allow for the rapid integration of detection, anti-drone, and smart ammunition systems with AI capabilities (Smid, Mărgăritescu, 2025).

The stimulation of RDI and digitization is reflected in the adoption of solutions for the SMART management of all defence resources, the use of virtual or augmented reality in training, and the creation and implementation of innovation ecosystems and centres of technological excellence at the national or regional level.

PERSPECTIVES OF AI IN DEFENCE RESOURCE MANAGEMENT

The evolution of AI opens new horizons in terms of defence resource management, at the strategic, operational, and tactical levels. In the coming years, AI will have a decisive influence on all components of the military spectrum, from decision-making processes to critical infrastructure security and the development of a digitalised defence doctrine (MSS Defence, 2025; Parangat, 2025).

AI capabilities based on Big Data and predictive models will continue to transform the military decision-making chain, enabling rapid scenario simulation, anticipation of emerging risks, and generation of adaptive interventions in theatres of operations. Systems such as Decision Support System (DSS) or Digital Twins for strategic simulation will provide military decision-makers with real-time data, reducing human error and accelerating adaptation to new types of conflict (Dragomir, 2025; Futures Platform, 2025). At the same time, AI will be increasingly used to merge and integrate data obtained from OSINT, SOGINT, and HUMINT sources, maximizing the information advantage (NATO ACT, 2025).

A major trend is the proliferation of autonomous systems (drones, ground vehicles, and integrated sensors, etc.) capable of executing complex missions without direct human interaction (MSS Defence, 2025; Parangat, 2025). Swarm Intelligence, in particular, will enable simultaneous operations with distributed forces and resources, increasing resilience, adaptability to mission and operating space specifics, and significantly reducing personnel exposure in hostile environments. Connecting these systems to edge computing networks and satellites will provide real-time defense on all fronts: land, air, sea, space, and cyber (SmartDev, 2025).

Sustainability is becoming a priority, with AI being the tool that will reduce resource consumption, optimize logistics and infrastructure maintenance, ensuring both budgetary efficiency and a low environmental footprint. (Parangat, 2025; SmartDev, 2025). Through SMART management of energy and material consumption in military installations, AI systems will directly contribute to the transition to green defense, in line with EU and NATO strategies (MEAT, 2024).

The development of public-private partnerships and national RDI ecosystems will enable not only the rapid adoption of technological advances but also digital sovereignty and strengthened international cooperation (ADR, 2024). Defense-as-a-Service (DaaS) models, including satellite services or ISR platforms, will make management processes more flexible, scalable, and financially predictable (MSS Defence, 2025).

The most challenging perspective remains that related of AI governance and regulation at all levels and in all areas of society. The need for transparency, algorithmic accountability, and ethical control is more acute now that decision-making is increasingly delegated to machines. Specialists from various fields are now proposing the development of an internationally applicable legal framework to sanction abuses and manage the moral dilemmas of AI and autonomous lethal force (Universul Juridic, 2025; European Parliament, 2025).

AI will not automatically resolve tensions in the security environment, but it will certainly be the key to future military superiority, allowing states that integrate it effectively to react adaptively, protect themselves intelligently, and anticipate new paradigms of hybrid warfare.

CONCLUSIONS

The article demonstrates that artificial intelligence has established itself as a strategic transformative vector in defence resource management, driving the efficiency, adaptability, and resilience of modern military systems. The integration of AI into defence resource management processes balances the need for rapid decision-making with the increasingly stringent requirement for security. Through automation, big data analysis, simulation, and autonomy, military structures have gained the ability to react proactively and adaptively, to manage complex scenarios, and to continuously innovate under the pressure of global competition and emerging crises.

The benefits offered by AI – cost reduction, increased response speed, transition to predictive and proactive operational models – are already being realized in military practice, both nationally and internationally. The automation of logistics processes with AI, rapid detection of vulnerabilities, optimization of all types of resources, and algorithm-assisted decision-making are becoming not only opportunities but also standard operational requirements.

At the same time, the expansion of AI also brings several significant challenges: cybersecurity risks, dependence on complex infrastructures, an acute need for ethics and algorithmic governance, and the risk of autonomous decision-making errors with strategic impact. The depersonalization of decision-making and the delegation of critical tasks to AI agents make it imperative to maintain ultimate human control and implement a robust legal framework to prevent abuses and incidents with lethal or serious geopolitical potential.

The future belongs to those military and civilian organizations that demonstrate flexibility, innovation, and the ability to ensure human-machine interoperability

in a transparent, responsible, and legally validated manner. Continued investment in R&D, international collaboration, and the development of human skills to understand and manage AI will be key to maintaining information superiority and strategic and technological resilience in the context of the accelerated evolution of digital warfare.

BIBLIOGRAPHY:

1. Acquah, E. (2025). *How to Apply AI in Military and Defense Projects: Inside the Systems Powering Modern Warfare*, <https://www.dartai.com/blog/how-to-apply-ai-in-military-and-defense-projects>, retrieved on 14 June 2025.
2. Army.mil. (2025-a). *Cyber key to protecting critical infrastructure, preparing Army for future fight*, https://www.army.mil/article/288466/cyber_key_to_protecting_critical_infrastructure_preparing_army_for_future_fight_pugh_says, retrieved on 18 July 2025.
3. Army.mil. (2025-b). *Empowering Sustainment Through Financial Excellence*, https://www.army.mil/article/282487/empowering_sustainment_through_financial_excellence, retrieved on 21 August 2025.
4. Autoritatea pentru Digitalizarea României (ADR) (2024). *Strategia Națională în domeniul inteligenței artificiale 2024-2027*, <https://www.adr.gov.ro/wp-content/uploads/2024/06/Strategia-Nationala-pentru-Inteligenta-Artificiala.pdf>, retrived on 23 June 2025
5. Bertalanffy, L. von. (1968). *General system theory: Foundations, development, applications*. New York: George Braziller, https://monoskop.org/images/7/77/Von_Bertalanffy_Ludwig_General_System_Theory_1968.pdf, retrieved on 14 June 2025.
6. Bonnemaïson, A. (2025). *AI for Defensive Cyber Operations*. *Trends Research & Advisory, Issue 614*, https://trendsresearch.org/pdf/AI-for-defensive-cyber-operation-En.pdf?srsItd=AfmBOoohjdbOjfvzxaTID_ArIRR4mReBnAfu9Qqc8jcJFf26m_Vbc4wN, retrieved on 14 June 2025.
7. Cernăianu, A. (2006). *Considerații privind infrastructura teritorială și militară a României în contextul deplinei integrări a țării în NATO*, in *Buletinul Universității Naționale de Apărare "Carol I"*, vol. 2, p. 29, <https://buletinul.unap.ro/pdf/buletin-2-2006.pdf>, retrieved on 14 June 2025.
8. Construct Intelligence (2025). *Investițiile în infrastructura militară accelerează pe fondul crizei din Est*, <https://construct-intelligence.ro/investitiile-in-infrastructura-militara-accelereaza-pe-fondul-crizei-din-est-analiza/>, retrieved on 10 September 2025.
9. Daniels, M. (2025). *Combining AI, Automation Creates Mission Efficiency*, <https://www.nationaldefensemagazine.org/articles/2024/8/28/industry-perspective-combining-ai-automation-creates-mission-efficiency>, retrieved on 14 June 2025.
10. DARPA (2025). *Securing Artificial Intelligence for Battlefield Effective Robustness*, <https://www.darpa.mil/sites/default/files/attachment/2025-03/program-darpa-saber-proposer-day-presentation.pdf>, retrieved on 18 July 2025.
11. Datategy (2025-a). *How AI Transforms Predictive Maintenance in Defense Equipment*, <https://www.datategy.net/2025/07/01/how-ai-transforms-predictive-maintenance-in-defense-equipment/>, retrieved on 18 July 2025.

12. Datategy (2025-b). *How to Orchestrate AI Deployment in Defense Infrastructures*, <https://www.datategy.net/2025/07/16/how-to-orchestrate-ai-deployment-in-defense-infrastructures/>, retrieved on 18 July 2025
13. Davis, F.D. (1989). *Perceived usefulness, perceived ease of use, and user acceptance of information technology*. *MIS Quarterly*, 13(3), pp. 319-340, https://www.researchgate.net/publication/200085965_Perceived_Usefulness_Perceived_Ease_of_Use_and_User_Acceptance_of_Information_Technology, retrieved on 12 September 2025.
14. Decker, A. (2024). *Can AI reduce Air Force logistics planning from days to minutes?*, <https://www.defenseone.com/threats/2024/02/can-ai-reduce-air-force-logistics-planning-days-minutes/393850/>, retrieved on 23 June 2025.
15. Defense Logistics Agency (DLA) (2025). *Utilization of Artificial Intelligence (AI) to Illuminate Supply Chain Risk*, <https://www.dla.mil/About-DLA/News/News-Article-View/Article/4186367/utilization-of-artificial-intelligence-ai-to-illuminate-supply-chain-risk/>, retrieved on 18 July 2025.
16. Dragomir, C. (2025). *Integrarea inteligenței artificiale în managementul resurselor pentru apărare. Integrarea inteligenței artificiale în cercetarea operațională*, in *Gândirea Militară Românească*, no. 1/2025, <https://gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20GMR/2025/1/DRAGOMIR-1.pdf>, retrieved on 10 September 2025.
17. European Court of Auditors (ECA) (2019). *European Defence*, https://www.eca.europa.eu/lists/ecadocuments/rew19_09/rew_eu-defence_en.pdf, retrieved on 21 August 2025.
18. European Parliamentary Research Service (EPRS) (2025). *Defence and artificial intelligence*, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769580/EPRS_BRI\(2025\)769580_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769580/EPRS_BRI(2025)769580_EN.pdf), retrieved on 21 August 2025.
19. EY (2025). *Smart Arsenal: The Role of AI in Military Asset Management*, https://www.ey.com/en_us/insights/government-public-sector/the-role-of-ai-in-military-asset-management, retrieved on 18 July 2025
20. FlySight. (2023). *Artificial Intelligence in Military Technology - 8 Applications Examples*. <https://www.flysight.it/artificial-intelligence-in-military-technology-8-applications-examples/>, retrieved on 14 June 2025.
21. Fortinet (2024). *Artificial Intelligence (AI) in Cybersecurity: The Future of Defense*, <https://www.fortinet.com/resources/cyberglossary/artificial-intelligence-in-cybersecurity>, retrieved on 12 September 2025.
22. Futures Platform (2025). *AI is already changing defence planning. Can oversight keep up?*, <https://www.futuresplatform.com/blog/artificial-intelligence-military-defence-market-data-future-trends>, retrieved on 14 June 2025.
23. IBM (2025). *IBM Maximo for Defense*, <https://www.ibm.com/products/maximo>, retrieved on 14 June 2025.
24. Ilie, A.M. (2024). *Sistemul logistic integrat*, https://codrm.eu/wp-content/uploads/2024/12/07_Ilie_Ana_Mona.pdf, retrieved on 18 July 2025.
25. Infosys BPM (2025). *AI and Autonomous drone technology in logistics*, <https://www.infosysbpm.com/blogs/travel-hospitality/ai-drones-revolutionising-delivery-and-transportation.html>, retrieved on 23 June 2025.

26. Jianu, F. (2014). *Particularitățile managementului resurselor specifice afacerilor militare*, in *Buletinul Universității Naționale de Apărare "Carol I"*, no. 4, pp. 161-164, <https://revista.unap.ro/index.php/revista/article/download/67/50/0>, retrieved on 10 September 2025.
27. Johnson, J. (2019). *Artificial intelligence future warfare: Implications for international security*. *Defense Security Analysis*, 35(2), pp. 147-169, <https://doi.org/10.1080/14751798.2019.1600800>, retrieved on 21 August 2025.
28. King, A. (2024). *Digital Targeting: Artificial Intelligence, Data, and Military Strategy*, in *Journal of Global Security Studies*, 9(2), https://ore.exeter.ac.uk/articles/journal_contribution/Digital_Targeting_Artificial_Intelligence_Data_and_Military_Intelligence/29806868?file=56852888, retrieved on 23 June 2025.
29. Maathuis, C., Cools, K. (2025). *The Role of AI in Military Cyber Security: Data Insights and Challenges*, *Procedia Computer Science* Volume 254, pp. 191-200, <https://www.sciencedirect.com/science/article/pii/S1877050925004284>, retrieved on 18 July 2025.
30. Markets and Markets (2025). *AI's Role in World Defense Budget Market*, <https://www.marketsandmarkets.com/ResearchInsight/ai-impact-analysis-on-world-defense-budget-industry.asp>, retrieved on 21 August 2025.
31. Mayer, M. (2023). *Trusting machine intelligence: Artificial intelligence and human-autonomy teaming in military operations*, in *Defense Security Analysis*, 39(4), pp. 521-538, <https://www.tandfonline.com/doi/full/10.1080/14751798.2023.2264070#d1e121>, retrieved on 18 July 2025.
32. McKinsey&Co. (2025). *AI is the greatest threat – and defense – in cybersecurity today. Here's why*, <https://www.mckinsey.com/about-us/new-at-mckinsey-blog/ai-is-the-greatest-threat-and-defense-in-cybersecurity-today>, retrieved on 14 June 2025.
33. Mihălțianu, A. (2025). *ReArmRomânia: cum să-ți modernizezi Armata să fie gata de luptă când deficitul tău bugetar de 9.3% e cel mai mare din Europa*, <https://pressone.ro/rearm-romania-cum-sa-ti-modernizezi-armata-sa-fie-gata-de-lupta-cand-deficitul-tau-bugetar-de-9-3-e-cel-mai-mare-din-europa>, retrieved on 18 July 2025.
34. Ministerul Economiei, Antreprenoriatului și Turismului (MEAT) (2024). *Strategia Națională pentru Industria de Apărare 2024-2030*, <https://sgg.gov.ro/1/wp-content/uploads/2024/11/ANEXA-44.pdf>, retrieved on 10 September 2025.
35. MSS Defence (2025). *Apărare 2025: Principalele tendințe care conduc la inovare*, <https://mssdefence.com/ro/blog/apararea-2025-principalele-tendinte-care-determina-inovarea/>, retrieved on 23 June 2025.
36. Mustăț, A., Jude, C. (2023). *Utilizarea inteligenței artificiale pentru operaționalizarea militară*, https://www.aosr.ro/wp-content/uploads/2023/01/Mustata_Jude_Raport-Cercetare-AOSR-Decembrie.pdf, retrieved on 14 June 2025.
37. NATO Allied Command Transformation (ACT) (2025). *Harnessing Artificial Intelligence*, <https://www.act.nato.int/article/harnessing-artificial-intelligence/>, retrieved on 18 July 2025.
38. Nilsson, N.J. (2009). *The quest for artificial intelligence: A history of ideas and achievements*, Cambridge University Press, <https://ai.stanford.edu/~nilsson/QAI/qai.pdf>, retrieved on 18 July 2025.
39. Palantir (2025-a). *Apollo Defense Solutions*, <https://www.palantir.com/solutions/defense/>, retrieved on 14 June 2025.

40. Palantir Technologies (2025-b). *Gotham Intelligence Platform*, <https://www.palantir.com/>, retrieved on 14 June 2025.
41. Parangat (2025). *How Artificial Intelligence (AI) is Evolving the Future of Military Defense Approaches*, <https://www.parangat.com/how-artificial-intelligence-ai-is-evolving-the-future-of-military-defense-approaches/>, retrieved on 23 June 2025.
42. Parlamentul European (2025). *Inteligența artificială: oportunități și pericole*, <https://www.europarl.europa.eu/topics/ro/article/20200918STO87404/inteligena-artificiala-oportunitati-si-pericole>, retrieved on 21 August 2025.
43. PwC (2025). *The global AI race and defense's new frontier*, <https://www.strategyand.pwc.com/de/en/industries/aerospace-defense/ai-in-defense.html>, retrieved on 18 July 2025.
44. RAND (2025). *Defense infrastructure*, <https://www.rand.org/topics/defense-infrastructure.html>, retrieved on 18 July 2025.
45. Rashid, A.B., Kausik, A.K., Sunny, A.A.H.&Bappy, M.H. (2023). *Artificial intelligence in the military: An overview of the capabilities, applications, and challenges. International Journal of Intelligent Systems*, https://www.researchgate.net/publication/375437930_Artificial_Intelligence_in_the_Military_An_Overview_of_the_Capabilities_Applications_and_Challenges, retrieved on 10 September 2025.
46. Russell, S., Norvig, P. (2016). *Artificial Intelligence: A Modern Approach* (3rd ed.). Pearson, https://api.pageplace.de/preview/DT0400.9781292153971_A27091185/preview-9781292153971_A27091185.pdf, retrieved on 23 June 2025.
47. SAP (2025). *SAP Integrated Logistics*, <https://www.sap.com>, retrieved on 14 June 2025.
48. Sarjito, A. (2024). *The Impact of Intelligence Gathering, Risk Analysis, and Scenario Planning on Defense Policy Formulation. International Journal Administration, Business Organization*, 5(3), pp. 27-46, <https://ijabo.a3i.or.id/index.php/ijabo>, retrieved on 12 September 2025.
49. Shaw, J. (2024). *Achieving Information Dominance in Military Applications through AI Sensor Fusion, Networking, Precision Timing and Advanced Computing*, <https://www.trentonsystems.com/en-us/resource-hub/blog/achieving-information-dominance-in-military-applications-through-ai-sensor-fusion-networking-precision-timing-and-advanced-computing>, retrieved on 23 June 2025.
50. Singh, R.K. (2025). *Defence secretary pushes AI-driven overhaul of armed forces financial systems*, <https://www.theweek.in/news/defence/2025/04/09/defence-secretary-pushes-ai-driven-overhaul-of-armed-forces-financial-systems.html>, retrieved on 10 September 2025.
51. SmartDev (2025). *AI in Military: Top Use Cases You Need To Know*, <https://smartdev.com/kr/ai-use-cases-in-military/>, retrieved on 14 June 2025.
52. Smid, S. Mărgăritescu, Șt. (2025). *Valorificarea potențialului României în domeniul dronelor de apărare: De la achiziții strategice la inovație locală*, <https://blog.pwc.ro/2025/05/20/valorificarea-potentialului-romaniei-in-domeniul-dronelor-de-aparare-de-la-achizitii-strategice-la-inovatie-locala/>, retrieved on 12 September 2025.
53. Soules, S., James, J., Hamrick, D., Van Blarcom, A. (2022). *Artificial Intelligence for Predictive Maintenance*, <https://www.boozallen.com/markets/defense/indopacific/artificial-intelligence-for-predictive-maintenance.html>, retrieved on 14 June 2025.

54. STS Romania (2023). *Logistica Militară: Coloana vertebrală a eficienței forțelor armate*, <https://stsromania.com/logistica-militara-coloana-vertebrala-a-eficientei-fortelor-armate/>, retrieved on 23 June 2025.
55. ThroughPut (2025). *Supply Chain Excellence for Mission Critical Operations*, <https://throughput.world/industries/military-and-defense/>, retrieved on 14 June 2025.
56. TMForum (2023). *AI-powered fraud defense: Turning vulnerability into profitability*, <https://www.tmforum.org/catalysts/projects/M24.0.701/aipowered-fraud-defense-turning-vulnerability-into-profitability>, retrieved on 10 September 2025.
57. Tookitaki (2025). *How AI-Powered Anti-Fraud Solutions are Strengthening Financial Security*, <https://www.tookitaki.com/compliance-hub/ai-powered-anti-fraud-solutions-are-strengthening-financial-security>, retrieved on 12 September 2025.
58. Trax Technologies (2025). *55 AI Models to Transform Military Supply Chain Operations*, <https://www.traxtech.com/ai-in-supply-chain/55-ai-models-to-transform-military-supply-chain-operations>, retrieved on 14 June 2025.
59. Universul Juridic (2025). *Priorități și perspective de dezvoltare ale dreptului inteligenței artificiale*, <https://www.universuljuridic.ro/prioritati-si-perspective-de-dezvoltare-ale-dreptului-inteligentei-artificiale/>, retrieved on 19 September 2025.
60. Verbitskaya, T. (2025). *The Future of Logistics. AI Drones Streamlining Delivery and Supply Chain Management*, <https://keymakr.com/blog/untitled-4/>, retrieved on 23 June 2025.
61. Webster, J.L., Reif, W.E., Bracker, J.S. (1989). *The manager's guide to strategic planning tools and techniques*, in *Planning Review*, 17(6), pp. 44-48. https://www.researchgate.net/publication/316603417_Strategic_Management_Tools_and_Techniques_Usage_a_Qualitative_Review, retrieved on 19 September 2025.
62. Wickens, C.D., Gordon, S.E., Liu, Y., Lee, J. (2004). *An introduction to human factors engineering* (2nd ed.). Pearson Prentice Hall, https://www.researchgate.net/publication/239060793_An_Introduction_to_Human_Factors_Engineering, retrieved on 23 June 2025.
63. Zentner, E. (2025). *Investing in Defense and Aerospace*, <https://www.morganstanley.com/articles/investing-in-defense-stocks>, retrieved on 14 June 2025.

THE NECESSITY OF IMPLEMENTING THE CONCEPT OF “MILITARY MOBILITY” AT THE NATIONAL LEVEL FOR THE DEPLOYMENT OF FORCES PARTICIPATING IN OPERATIONS BY LAND

Colonel Professor Dr. Alexandru HERCIU

“Carol I” National Defense University, Bucharest

Captain Ionela Cătălina MANOLACHE, Doctoral student

Headquarters Multinational Division South-East Bucharest

DOI: 10.55535/RMT.2025.3.31

Current threats to international security are stronger than at any point in recent history, and the member states of NATO and European Union have an obligation to take the most effective measures to protect their citizens. Defensive actions must be continuously conducted in order to prevent a potential state of conflict, and the development of military mobility by the member states represents an immediate task within the current international configuration. Each NATO and/or EU member state is responsible to implement, at the national level, projects and programs ensuring the rapid deployment of military equipment, vehicles and materials across the transatlantic space. Regardless of the nature of the operation, military forces must benefit from all necessary conditions, in terms of logistics and military mobility, to be deployed in a timely and secure manner anywhere within the territory of the allied or partner states.

Keywords: force deployment; military mobility; dual-use infrastructure; Security Action for Europe; interoperability;

INTRODUCTION

The reassessment of NATO and the EU’s capacity to defend against a possible military threat originating from the East has become a priority for these organizations, as well as for each individual state. The conflict provoked by Russia in Ukraine in February 2022, along with more recent geopolitical and geostrategic challenges, such as the redefinition of national objectives and priorities and the growing trends that elevate nationalism as primary resource in European political sphere (Lăzărescu 2024) represent significant security concerns that impact global peace and stability.

In the current situation, both NATO and the EU find themselves compelled to reorient their policies and ensure that they can fulfill their roles as structures able to generate security. Despite peace treaties and guarantees, Russia has always represented a source of danger and concern, particularly for the countries in its vicinity, located on the Eastern Flank of Europe. In order to adequately respond to the challenges and threats periodically posed by Russia, the two organizations have taken concrete measures to maintain security on their territory since February 2022.

On July 1, 2024, NATO, an alliance founded on the principles of deterrence and defense, completed its transition to a *new force structure (NATO Force Model)* (SHAPE Public Affairs Office, 2024): a multinational, highly technologized and readiness-oriented structure, capable of operating across all domains and deploying rapidly to any location. The decision to transform the NATO Response Force (NRF) into a new model was made at the 2022 Madrid Summit, with the goal of increasing the number of available and ready forces, to be used in the Allies’ defense plans (NATO 2025). Furthermore, NATO deployed four new battlegroups in Bulgaria, Hungary, Romania and Slovakia, in addition to the four already established in Poland and the Baltic States. These battlegroups are part of the enhanced Forward Presence (eFP), have brigade-level strength and consist of military forces contributed by member states on a rotational basis (Palavenis, 2025). These measures are intended to validate the Alliance’s strength and capability, yet they also place significant logistical pressure on the deployment of such a large number of forces.

Although the Alliance has revised its force employment plans precisely to demonstrate commitment and collective effort, the EU, in turn, has been compelled

to decide on rearmament and the strengthening of its military posture in the shortest time possible, as a result of the unpredictability of the United States (US) in which has been undergoing both internal and external transformations following the inauguration of the Donald Trump's administration (Naumescu, 2025).

As early as 2022, within the framework of the Strategic Compass, the European Union launched the idea of creating a European Union Rapid Deployment Capacity (EU RDC), designed to enable the organization to rapidly deploy up to 5.000 troops to participate in various types of operations (Meyer, Van Osch, Reykers, 2022). However, considering all recent security changes, the member states initiated the „ReArm EU” project, aimed at maintaining a safe and stable environment for citizens through military means, in the event of a deterioration of transatlantic relations and a reduction in the capacity of Western states to defend the Eastern Flank against Russian Federation (European Commission 2025). This plan, detailed in a key Union document: *White Paper for European Defence – Readiness 2030*, stipulates the use of available financial resources to mobilize up to 800 billion dollars in defense investments. The goal of the Readiness 2030 initiative is to ensure that the European defense industry possesses the capacity to produce armaments at a rate and scale consistent with current security requirements, as well as to facilitate the rapid deployment of forces across the entire European territory (Santopinto, 2025).

The measures adopted by NATO and the EU exemplify the current security environment and contribute to the evolution of military mobility not only at the multinational level, but also nationally, as each state acknowledges the necessity of developing procedures, projects and mechanisms to enable the rapid movement of forces across its territory, thereby ensuring their defense.

This paper aims to examine both these security aspects and the measures adopted by the two organizations to ensure them, while also substantiating the need to implement a coherent military mobility system in Romania, dedicated to land operations.

The analytical structure of this paper will begin with the establishment of a theoretical foundation in the field of military mobility, through the presentation of the main concepts, definitions and relevant distinctions. Subsequently, we will analyze the current state of military mobility implementation at the national level by assessing Romania's existing capabilities, identifying major disfunctions and highlighting concrete examples. Next, we will emphasize the necessity of integrating an efficient military mobility system by outlining the main advantages identified, as well as the associated risks. We will then formulate proposals for appropriate measures and policies, correlated with the data obtained from our analysis

and finally, we will draw relevant conclusions for this field. The entire study will be based on a research method appropriate to the proposed objectives> documentary analysis.

The sources in this research include scientific articles and studies by Romanian and foreign authors, books, reports, official statements and studies produced by NATO, the EU or agencies specializing in military mobility. In addition, military regulations with a low classification level are analyzed. Certain methodological limitations are anticipated, arising from the inaccessibility of sensitive military information due to the protection of ongoing projects.

THEORETICAL FOUNDATIONS OF MILITARY MOBILITY

Theoretically, an essential first step consists of defining the concept of military mobility in a broad sense. In general understanding, this term is associated with “*the ability to move military personnel and equipment over various distances, including across borders*” (Cokelaere, 2022). It is important to present this concept from the perspective of NATO and EU doctrines, as these definitions are universally accepted by all member states and reflect the shared vision in this field.

From the EU’s perspective, military mobility represents a current strategic challenge, linked to the need for the rapid and secure deployment of forces. According to the official definition, military mobility refers to “*the movement of military personnel and assets from one place to another, including cross-borders by using different modes of transport.*” (EDA, 2019).

In the context of the organization’s eastward expansion, the use of dual-use infrastructure and the reduction of bureaucratic obstacles are essential to ensure uniform economic, social and security conditions across the entire Union. The organization has been the main actor to recognize the importance of the rapid movement of forces and military equipment throughout its territory and has adopted a series of projects, regulations and initiatives aimed at optimizing the deployment process.

The European Union plays a major role in funding the development of dual-use infrastructure through the Connecting Europe Facility/CEF component, which aims to harmonize transport networks between the Western and Eastern, as well as the Northern and Southern regions (Bellomo, 2023).

Furthermore, the Security Action for Europe (SAFE) instrument, adopted on May 27, 2025 (European Union 2025), within the „ReArm” Europe program, provides member states with access to approximately 150 billion euros for urgent investments aimed at strengthening defense capacity. *Military mobility* has been

identified by the EU as a priority area to be addressed, fully or partially, through these funds. Projects related to force deployment, logistics and dual-use infrastructure can be implemented through the SAFE mechanism. For projects submitted by July 2025, Romania is expected to receive approximately 16.7 billion euros.

NATO likewise demonstrates an increased interest in this field and has launched several initiatives aimed at facilitating cross-border movements, reducing bureaucracy, increasing movement speed and standardizing transport infrastructure across the transatlantic area. In the context of intensified military exercises, particularly along the Eastern Flank, the importance of rapid force mobility has become increasingly evident, as military convoys often face challenges such as narrow roads, limited railway capacity, incompatible rail gauges or excessive administrative procedures. The interest in *military mobility* is also reflected at the doctrinal level, through its integration into operational concepts and strategic planning processes. In this regard, NATO defines military mobility as “a quality or capability of military forces which permits them to move from place to place while retaining the ability to fulfill their primary mission” (Ministry of Defence, 2021), a definition that generally reflects the EU’s approach.

Romania, as a member state of both the EU and NATO, aligns itself with the strategic directions promoted by these organizations in the field of *military mobility*. Thus, an increasing interest can be observed in implementing policies and initiatives focused on the development of dual-use transport infrastructure, the simplification of bureaucratic procedures, the digitalization of logistical processes and the use of emerging and disruptive technologies (EDT) aimed at optimizing military mobility.

Currently, at the doctrinal level, Romania does not have an official definition of the concept of *military mobility* and academic efforts dedicated to in-depth research in this field remain, for the time being, limited.

Returning to the theoretical foundation provided at the level of international organizations, it is essential to present and distinguish between the three types of military mobility: *strategic, operational and tactical*.

Strategic mobility is defined by NATO as “the capability to move forces and their associated logistics in a timely and effective manner over long distances. This could be between joint operations, areas, between regions, or beyond NATO’s area of responsibility.” (NATO, 2020). During the conduct of NATO operations, national military capabilities can be strengthened through multinational cooperation and commitment, support from multinational military agencies and collaboration with private entities. The success of operations depends on the quality and number

of embarkation and debarkation points within or from the deployment area, as well as on the efficiency of the transport infrastructure used (NATO, 2022). Strategic mobility refers to the projection of forces over long distances, typically between countries or continents.

Operational mobility refers to „the movement of forces between or within theatres of operations for the purpose of regrouping, reinforcing or repositioning forces in support of the conduct of a military campaign.” (NATO, Allied Joint Doctrine for the Conduct of Operations AJP-3 2019).

Tactical mobility is “the ability to move rapidly from one part of the battlefield to another, relative to enemy.” (Ib.). It is the closest to the commander’s immediate decision-making level and is essential for the success of a mission. Its effectiveness depends on rigorous planning that takes into account factors such as terrain topography, infrastructure condition and the technical and tactical characteristics of military equipment.

One of the main challenges hindering the military mobility of forces is critical infrastructure, particularly *transport infrastructure*. Current plans developed at the European and Euro-Atlantic levels focus precisely on the development of transport infrastructure and capabilities that are capable, secure, sustainable and resilient, in order to support weight, dimensions and scale of modern military equipment.

Modernizing dual-use transport infrastructure along the trans-European transport network (TEN-T), which spans the entire territory of the Union, is a priority to ensure that this network can support high-tonnage and complex military transports on short notice. Although Romania faces significant deficiencies in the quality of its transport network, particularly in the Eastern and Southern regions, it is making continuous efforts to address these gaps. According to the European Commission, Romanian authorities have accelerated the implementation of projects targeting dual-use military mobility to facilitate the rapid, efficient and coordinated movement of military equipment and personnel (Comisia Europeană, 2022). This course of action is essential for ensuring the optimal conduct of planned multinational military exercises on national territory, in accordance with the strategic agenda of the North Atlantic Alliance.

CURRENT STATE OF DUAL-USE MOBILITY, AT THE NATIONAL LEVEL

Romania is an European state that, due to its geographic position, possesses all major forms of transport: road, rail, air, maritime, inland waterways and intermodal. However, the degree of implementation, interconnection and modernization of its transport network has not progressed at the pace required by emerging security challenges and contemporary operational dynamics.

With a significant geostrategic position within the EU and NATO, Romania has become a key focus for the development of dual-use transport networks, both for national authorities and for allied or partner states. In this context, the number of infrastructure projects compatible with the TEN-T network requirements, as well as with the specific needs of military mobility, has increased. These projects contribute to facilitating the rapid access of foreign military forces anywhere within national borders, strengthening the Alliance's response capability in the region.

From the perspective of *road infrastructure*, the latest statistics from 2024 show that the public road network totals nearly 88.000 km, of which over 1.300 km are highways and expressways, more than 17.600 km are national roads, over 35.000 km are county roads and the remainder are communal roads (Pislaru, 2024). Due to funding for infrastructure expansion allocated both from the EU budget and the national budget, Romania's infrastructure has begun to provide much better connectivity between the country's regions, although some projects still need completion, particularly in the Moldavia region and in the southwestern part of the country. In the current geopolitical and strategic context, the road network is essential for NATO forces' military mobility, logistic transit for the Eastern Flank and the increased frequency of international military exercises and transports.

From the perspective of *rail infrastructure*, Romania faces a high degree of technological wear. Most of the national railway network was built during the communist era and modernization efforts in recent decades have been limited and sporadic. Currently, the network extends over 10.000 km, but only approximately 4% is electrified, placing Romania well below the European average in terms of quality and performance of the rail transport system. For example, the average commercial speed for freight transport is about 15 km/h, while for passenger transport it is 45 km/h. In contrast, the EU average is 45 km/h for freight and 123 km/h for passengers (Mușat, 2023). Nevertheless, Romanian authorities are attempting to revitalize the railway sector, particularly in terms of its capacity to support dual-use mobility. A recent example is the launch of CarpatiaFeroviar SA (Horpeniakova, 2024), a company dedicated to freight transport with dual-use capabilities. In addition, a process has been initiated to replace aging train units with modern ones, adapted to both domestic and European interoperability requirements.

From the perspective of *air infrastructure*, Romania is in a significantly more favorable position compared to other modes of transport. Nationally, 28 aerodromes and 6 heliports are operational, strategically distributed across the country, allowing for both cargo and passenger transport, including in the context of strategic logistical operations. The largest national airport is Bucharest "Henry Coandă" International

Airport, which has undergone extensive modernization to align with international standards. Romania, like other EU members, participates in the Single European Sky ATM Research/SESAR program, which represents the technological and operational component of the Single European Sky/SES initiative. The program aims to integrate and optimize air traffic management through digitalization, interoperability and the use of advanced technologies, thus contributing to strengthening air security and mobility within the EU (ROMATSA, w.y.).

From the perspective of *maritime infrastructure*, Romania possesses significant strategic potential due to its direct access to the Black Sea and its favorable position along international transport routes. Constanța, Mangalia and Midia are three major seaports, each playing a complementary role in managing cargo, passenger traffic and industrial activities.

Constanța Port is the largest national port and one of the most important in Eastern Europe, due to its logistics capacity and intermodal connections. It serves as a strategic entry point for commercial flows to and from the EU and is connected to the central network of the TEN-T Rhine-Danube corridor. In recent years, Romanian authorities have launched major investments projects to modernize port infrastructure, which had been neglected in the post-communist era. These initiatives aim to increase operational capacity, digitalize logistical processes and adapt ports to new security and energy-efficiency (Drăgan, Olteanu, Stângă, 2022). Given its European commitments, Romania is obliged to align its maritime infrastructure with EU standards, particularly regarding dual-use infrastructure and the support of mobility in the Black Sea region.

From the perspective of *inland waterway infrastructure*, Romania has a geographical advantage due to the Danube River, which crosses the national border from West to East over a length of 1.075 km. along this segment, several strategically important river ports are located, enabling commercial and logistical activities. Additionally, there are approximately 1.500 km of other navigable inland waterways (secondary branches of the Danube, the Danube-Black Sea Canal, the Poarta Albă-Midia-Năvodari Canal and the Bega Canal), which contribute to an extensive navigable infrastructure with dual-use potential.

Although during dry summer periods river transport faces challenges, if authorities ensure proper maintenance, dredging and modernization of the inland waterway infrastructure, this sector can be used not only for civilian cargo transport, but also as an additional route for moving military equipment and assets, particularly in the context of the need for diversified and redundant logistics at the regional level (Păvălașc, 2022).

From the perspective of *intermodal infrastructure*, Romania is undergoing a process of expansion and consolidation of this essential component of modern logistical mobility. Its favorable geographical position at the intersection of key European corridors, provides the country with significant potential for developing intermodal hubs, particularly through the integration of road, rail, air, maritime and inland waterway transport. Direct access to the Black Sea, via the Port of Constanța, strengthens Romania's role within the TEN-T and facilitates the integration of international logistical flows. The intermodal network is aligned with the TEN-T corridors crossing the national territory: Rhine-Danube and Orient-East Med.

Nowadays, many of the intermodal terminals in operation or under development are managed by private operators, investing in modern logistics platforms near major transport arteries. At the same time, national authorities have begun supporting the development of integrated logistics centers through EU-funded projects. This evolution confirms the importance of intermodal infrastructure as a key element of dual-use mobility, capable of supporting both civilian trade requirements and the operational needs of military mobility in the European context.

Although substantial efforts have been made in recent years to develop dual-use infrastructure on national territory, in line with international commitments, domestic economic realities continue to limit the pace of implementation. In this context, a number of structural and administrative dysfunctions persist, which affect the efficiency of military mobility within national borders.

Firstly, the issue of *functional interoperability between civilian and military structures* has not yet been resolved. Although military mobility has become an increasingly prominent topic on the national security agenda, there is currently no coherent standardization of the relationship and cooperation procedures between the Ministry of National Defense (MoD) and other institutions responsible for transport and logistics infrastructure, such as Ministry of Transport and Infrastructure (MTI), the Ministry of Digitalization, the Ministry of Finance or other private-sector actors. In the absence of a consolidated regulatory framework, information exchange and inter-institutional coordination are carried out primarily at the initiative of MoD, through ad-hoc mechanisms such as interministerial working groups, cooperation protocols, administrative arrangements or bilateral agreements. In times of crisis, this reactive and fragmented approach limits rapid response capability and reduces the overall efficiency of dual-use infrastructure.

Secondly, the remains of *a high level of bureaucracy* in the approval of military transports, particularly foreign ones. In the event of a conflict or crisis on the Eastern Flank, the Alliance's ability to rapidly deploy forces, equipment and military

materials to the area of interest is vital to ensuring an effective response. Currently, however, the administrative procedures and authorizations required for foreign military convoys to transit national territory are cumbersome, fragmented and uncoordinated. Oversized transports, such as tanks or artillery systems, must go through a series of customs and security formalities. These issues highlight the urgent need for harmonization and standardization so that cross-border transfer can be carried out quickly, safely and efficiency in the event of an operational emergency.

Thirdly, there are *no officially designated military routes* for the movement of military convoys on national territory. Military transports are carried out predominantly along the TEN-T corridors. However, these corridors also serve civilian freight and passenger traffic. Although the corridors meet over 94% of military requirements, frictions still exist regarding the special transport needs of certain oversized equipment, substances that must be transported under specific conditions or equipment that must be moved as quickly as possible to particular locations. Civilian traffic or restrictions on certain segments can pose obstacles. Therefore, identifying, testing and marking routes suitable for military mobility, along with establishing civil-military coordination mechanisms for their allocation would represent an important step toward increasing operational efficiency.

Eloquent examples highlighting dysfunctions in military transport on national territory are the case of the Ungheni Bridge (at Romania’s border with the Republic of Moldova) and the railway bridge at Negru Vodă.

The road and railway bridge at Ungheni holds significant strategic importance for military mobility within the national territory. It serves as a strategic link between Romania and the Republic of Moldova, facilitating the rapid transit of troops and military equipment between the two states. The bridge is part of the military mobility infrastructure and supports the conduct of exercises and international military cooperation, by providing direct connectivity with Moldova for joint Romanian-Moldovan or international exercises. Despite its importance, the construction of the bridge has been delayed. Its connection to the existing infrastructure is uncertain (the bridge will be part of the A8 highway, but the final route of it links to other roads and other connections are not fully established). Feasible timelines for execution and operation are unrealistic, the size and capacity may be limited for certain scenarios and building it at the border presents logistical and security challenges (Borcea, 2025).

The railway bridge at Negru Vodă, located along the route toward the Smârdan training area currently does not meet the requirements for military mobility.

During the NATO exercise Steadfast Dart 2025, held in January-February 2025, infrastructure limitations were reported: several military convoys of allied forces could not cross the bridge according to the planned itinerary, due to insufficient vertical clearance that prevents the passage of large combat vehicles. Consequently, the participating units which were testing the rapid reaction capability of forces were redirected along an alternative route via the Vama Veche border crossing. However, this route is significantly closer to the Black Sea coast and, in the event of a real scenario, may involve an increased operational risk in terms of vulnerability to attack (Matei, Angelescu, 2025).

ARGUMENTS FOR THE DEVELOPMENT OF AN EFFECTIVE MILITARY MOBILITY SYSTEM

In the context of implementing a collective defense system within the transatlantic space, the need for an integrated transport network, characterized by synchronization, coordination and joint monitoring among allied and partner states has become increasingly evident. For Romania, to become a fully integrated actor in international initiatives concerning *military mobility* it must follow a common path with other states and adhere to infrastructure development projects aimed at reducing bureaucratic barriers. From a strategic perspective, mobility brings a series of advantages, such as enhancing the rapid reaction of forces, reducing vulnerabilities, optimizing logistical processes and strengthening Romania's credibility within NATO and the EU.

The rapid reaction of forces refers to the ability of armed forces to be deployed within a short period of time to areas where they are needed, particularly in emergency situations, with the aim of deterring or countering potential acts of aggression (Becker, Schulte, 2021). This capability depends on the existence of a modern, interconnected and functional transport infrastructure within each European state. Otherwise, even well-trained and well-equipped forces may face major challenges in terms of mobility, leading to delays in operations and, consequently, increased vulnerabilities and security risks. At the same time, the presence of a rapid reaction force on the Eastern Flank ensures regional stability, sends a deterrent message to potential adversaries and enhances the interoperability of forces.

Reducing vulnerabilities through the implementation of an effective military mobility system allows the dispersion of one's own, allied or partner forces located on national territory to different areas for the conduct of planned missions and activities without concentrating troops in fixed locations that could expose them to hostile attacks. When provided with adequate and continuous logistical support,

the ground transport of military forces can be carried out under optimal conditions, within the established timeframes and in accordance with mission specifications.

Optimizing logistical processes through improved military mobility is reflected in the ability to rapidly and efficiently support forces on the move by ensuring the timely delivery of critical resources necessary for mission success. This operational efficiency translates into reduced supply times, increased flexibility in the deployment of resources, decreased dependence on fixed logistical points, which can be vulnerable in the current context, and at the same time, lower costs associated with logistical support.

Strengthening national credibility within NATO and the EU is directly conditioned by Romania’s ability to ensure the rapid mobility of its own, allied or partner troops. This capability reflects the level of strategic commitment and the seriousness with which the Romania assumes its responsibilities. The state consolidates its position as a reliable partner if it can support the conduct of joint exercises by effectively managing all logistical, bureaucratic and administrative implications. Moreover, the recent commitments in the development of transport corridors together with neighboring states represent evidence of the involvement in regional projects aimed at expanding and modernizing infrastructure dedicated to military mobility (European Defence Agency, 2023).

If the state does not act quickly and in coordination with its partners to develop military mobility, a number of *risks* may arise, that could turn into threats to national security, such as delays in the execution of operations, endangerment of missions and the weakening of international cooperation.

The absence of an efficient military mobility system may lead to *delays in the execution of operations*, which risks resulting in the loss of tactical initiative, delayed defense of vulnerable areas and the inability to provide timely support from allied forces. In the current context, characterized by dynamism and the need for rapid responses, such deficiencies can seriously compromise the effectiveness and cohesion of collective action.

In the absence of adequate infrastructure, there is a risk of *jeopardizing missions*, which translates into exposing forces to unforeseen dangers, especially in situations where they are forced to use unsuitable routes or unprepared infrastructure. In such cases, the consequences can be severe, such as the compromise of strategic objectives if forces arrive too late to protect them, or the improper deployment of troops in areas of interest (Chifu, 2021).

The weakening of international cooperation can directly affect national security, as Romania has the obligation to align with the Euro-Atlantic strategic direction.

This responsibility entails concrete commitments: financial, human and institutional, to ensure mobility, security and the logistical support required for forces carrying out missions on national territory (Ioniță, 2020).

Given the threats and risks identified above, it is evident that the adoption of permanent and functional mechanisms to regulate the deployment of military forces is vital, in order to ensure a rapid response in the event of a conflict or crisis on the Eastern Flank of the Alliance. These mechanisms would reduce the forces' reaction times by implementing pre-established, standardized procedures or plans, facilitate the smooth execution of military operations through pre-approved action plans, enhance interoperability among NATO member states and enable better planning of logistical support.

NATIONAL MEASURES FOR FACILITATING MILITARY MOBILITY

Taking into account the aspects analyzed above, we consider that viable solutions exist for implementing the concept of *military mobility* at the national level. The proposed measures primarily aim to strengthen Romania's internal capabilities, while also generating positive effects internationally by directly contributing to NATO's and the EU's collective efforts in the field of *military mobility*. In this regard, we propose the following courses of action:

- Development and adoption of a clear, coherent and enforceable legislative framework at the national level, specifically regulating aspects of military mobility;
- Intensification of inter-institutional cooperation, both at the governmental level and through active involvement of the civilian sector, particularly in the area of critical infrastructure;
- Continuation of the growth rate of investments in dual-use infrastructure;
- Expansion and diversification of military exercises aimed at testing rapid reaction capability, interoperability and the mobility of forces within the national territory.

The development and adaptation of a clear legislative framework for military mobility is a vital measure for the continuation and efficiency of projects in this field. In this regard, it is necessary that all institutions involved in ensuring national defense and in facilitating or implementing projects related to transport infrastructure, as well as civil authorities, collaborate according to clear, uniform and well-structured rules. Ministries such as the Ministry of National Defense, Ministry of Transport and Infrastructure, Ministry of Finance, Ministry of Internal Affairs, Ministry of Digitalization, Ministry of European Projects Implementation

and Ministry of Development must cooperate institutionally, following *common procedures or regulations* when executing any project related to military mobility. Complementing this inter-institutional framework, the involvement of the private sector becomes increasingly relevant. Transport companies, developers of artificial intelligence-based autonomous systems and manufacturers of dual-use vehicles should be integrated into cross-sectoral working groups, through the designation of representatives with access to project-related information. Such an approach would contribute to increased transparency, decision-making efficiency and interoperability between institutional actors and the private sector.

Inter-institutional collaboration and the integration of the civilian component cannot remain a mere proposal: it must materialize through the creation of effective cooperation mechanisms between state institutions and private sector actors. In this regard, it is necessary to establish a framework for dialogue and coordination, allowing the active participation of all relevant parties in the planning, design and implementation stages of strategic infrastructure projects.

For example, in the development of a highway, the MoD should be consistently represented within interministerial working groups to communicate operational requirements, specific military transport needs and technical standards that should be applied. Such an approach would ensure the compatibility of civilian infrastructure with military mobility needs, while simultaneously reducing the risks associated with later adaptations and ensuring the efficient use of resources.

Increasing investments in dual-use infrastructure is a fundamental requirement for the future of military mobility, not only in Romania, but across Europe. Although the Romanian state allocates its own budgetary resources for infrastructure development, a significant share of funding comes from non-reimbursable European funds, particularly through the Connecting Europe Facility (Transport Component), and more recently through the SAFE mechanism. This component provides support from the military mobility envelope, amounting to 1.69 billion for EU member states, under which financing covers up to 50% of eligible expenses (Ministerul Transporturilor și Infrastructurii, 2023). Meanwhile, SAFE contributes to infrastructure enhancement, as over 30% of the projects submitted by Romania are dedicated to military improvements and are expected to receive funding (Dumitrescu, 2025), thereby facilitating military transport along routes soon to become operational. Additionally, NATO and the US, through funding under the NATO Security Investment Programme/NSIP and the European Deterrence Initiative/EDI, provide avenues for revitalizing Romania’s critical infrastructure.

With appropriate expertise, the Romanian state could attract substantial amounts from these programs to rebuild and modernize its transport network, ensuring that it meets dual-use transport requirements.

The multiplication and diversification of multinational exercises represent an essential measure for strengthening military mobility in the current context. An analysis of recent trends reveals the planning of exercises aimed at simulating allied intervention to halt a potential conflict on NATO's Eastern Flank, while simultaneously assessing the mobility capabilities of forces within Eastern European states. These countries, including Romania, continue to face infrastructural and administrative challenges that may hinder the efficient deployment of troops and equipment.

Romania has the opportunity to assume a regional leadership role in the organization and coordination of such exercises, by collaborating with neighboring states and other allies. This approach would not only allow for the testing and improvement of national capabilities, but also facilitate the attraction of funds aimed at developing dual-use infrastructure, which is essential for supporting military mobility. Furthermore, the annual planning of multinational exercises, such as Steadfast Defender, Dacian Spring or Dacian Fall can serve as a deterrent instrument against potential adversaries, while also enhancing interoperability and reducing reaction times in the event of regional crises.

CONCLUSIONS

In the current context of regional and international security, *military mobility* has become an essential pillar of collective defense both at the national level and within strategic alliances such as NATO and the EU. For Romania, the effective integration of military mobility requires not only alignment with international standards, but also the development of a coherent system adapted to national specificities.

Recently, Romania has made significant progress in this field. In July 2025, a portfolio of projects aimed at developing the defense industry and enhancing military mobility was submitted to the European Commission, with funding planned through the European SAFE mechanism. Approximately 30% of these projects focus on improving transport infrastructure and logistic connectivity, which are essential for the rapid deployment of forces. Moreover, Romania has signed regional agreements to develop military mobility corridors in collaboration with countries such as Bulgaria and Greece, aiming to simplify and accelerate the movement of troops and equipment along NATO's Eastern Flank.

Furthermore, within the multinational exercises planned for 2025, Romania demonstrated its commitment to strengthening military mobility. For example, Steadfast Dart 25 involved approximately 10.000 troops from 9 nations, testing rapid deployment capabilities and interoperability of allied forces on national territory.

In this context, Romania must adopt concrete measures to integrate military mobility into a coherent national system. This involves developing a clear legislative framework, intensifying inter-institutional and private sector collaboration, investing in dual-use infrastructure and organizing multinational exercises to test rapid deployment of forces. Only through the implementation of these measures can Romania strengthen its position as a reliable partner within NATO and the EU, thereby ensuring national security and contributing to regional stability.

Considering all the information presented so far, we conclude that developing a *national concept of military mobility* is absolutely necessary for Romania, as only an integrated strategic framework, encompassing legislative, logistical, dual-use infrastructure, civil-military cooperation and the adoption of emerging and disruptive technologies can ensure the rapid movement of forces in line with the commitments undertaken within NATO and the EU.

Given the relative novelty of this field, we propose that a future research direction should focus on the integration of artificial intelligence into this concept, as it could significantly enhance predictive analysis capabilities, optimal route planning, real-time logistical management and virtual simulations or exercises. These advancements would translate into shorter reaction times, improved interoperability and greater adaptability to unforeseen developments in the security environment.

BIBLIOGRAPHICAL REFERENCES:

1. *Allied Joint Doctrine for the Conduct of Operations AJP-3*. C. (2019). Brussels: NATO Standardization Office.
2. Becker, M., Schulte, B. (2021). “*Mobility and Military Logistics in Europe: Challenges and Solutions*”. *Stiftung Wissenschaft und Politik (SWP)*.
3. Bellomo, O. (2023). “*Bringing back military mobility*”. *Finabel – The European Army Interoperability Center*, pp. 1-9.
4. Borcea, Șt. (26 April 2025). *Adevărul*, <https://adevarul.ro/stiri-interne/societate/au-inceput-lucrarile-la-podul-pest-prut-de-la-2438989.html>, retrieved on 14 September 2025.
5. Chifu, I. (2021). “*România în arhitectura de securitate euroatlantică*”. Editura Institutului European din România.
6. Cokelaere, H. (2022). “*Ukraine war forces an EU rethink of military mobility*”, in *Politico*.

7. Cornea, O. (23 February 2025). *Europa Liberă*, <https://romania.europalibera.org/a/poduri-strategice-romania-nato-civil-militar-construcie-voila-cincu-brasov/33314879.html>, retrieved on 11 May 2025.
8. Drăgan, C., Olteanu, A.C., Stângă, V.G. (2022). "Strategic management of Constanța Port". *Postmodern Openings* 13, no. 1, pp. 105-123.
9. Dumitrescu, R. (30 July 2025). *Romania-Insider*, <https://www.romania-insider.com/romania-proposals-ec-safe-funding-jul-2025/>, retrieved on 10 September 2025.
10. European Commission (2022). "Joint Communication to the European Parliament and the Council on Military Mobility". Brussels.
11. European Commission (19 March 2025). *European Commission*, https://ec.europa.eu/commission/presscorner/detail/el/qanda_25_790, retrieved on 9 May 2025.
12. European Defence Agency (2023). *Military Mobility*, <https://eda.europa.eu/what-we-do/all-activities/activities-search/military-mobility>, retrieved on 10 May 2025.
13. European Union (2025). *Council Regulation (EU) 2025/1106 of 27 May 2025 establishing the Security Action for Europe (SAFE) through the Reinforcement of the European Defence Industry Instrument*. Council Regulation, Bruxelles: Publications Office of the European Union.
14. Horpeniakova, M. (18 October 2024). *RailMarket*, <https://railmarket.com/news/freight-rail/romania-replaces-cfr-marfa-with-a-new-rail-freight-operator-carpatica-feroviar>, retrieved on 9 May 2025.
15. Ioniță, S. (2020). "Logistica militară și infrastructura strategică: între planificare și reacție rapidă", in *Revista de Studii de Securitate*, no. 18, vol.2, pp. 45-62.
16. Lăzărescu, Al. (23 July 2024). *Revista 22*, <https://revista22.ro/opinii/alexandru-lazarescu/elitele-partidele-traditionale-si-extremistii>, retrieved on 10 May 2025.
17. Matei, C., Angelescu, P. (15 April 2025). *Știrile ProTV*, <https://stirileprotv.ro/stiri/actualitate/intamplare-jenanta-ce-au-patit-la-un-pod-in-jud-constant-trupele-nato-la-primul-mare-exercitiu-din-acest-an-din-romania.html>, retrieved on 9 May 2025.
18. Meyer, C., Osch, T. van, Reykers, Y. (2022). "The EU Rapid Deployment Capacity: This time, it's for real?", in *Policy Department for External Relations Directorate*, pp. 1-40.
19. Ministerul Transporturilor și Infrastructurii (2023). *Document sinteză privind politicile și programele bugetare pe termen mediu ale ordonatorilor principali de credite pentru anul 2024 și perspectiva 2025-2027*. București: Ministerul Transporturilor și Infrastructurii.
20. Ministry of Defence (2021). *Allied Joint Doctrine for the Deployment and Redeployment of Forces*, AJP-3.13. Allied Joint Publication, Bruxelles: NATO Standardization Office.
21. Mușat, C. (20 July 2023). *Gadget.ro.*, <https://gadget.ro/conform-unui-raport-oficial-cfr-viteza-medie-comerciala-a-trenurilor-de-marfa-in-2022-a-fost-de-15-6-km-ora/>, retrieved on 9 May 2025.
22. NATO (2022). *Allied Joint Doctrine for Movement* AJP-4.4. C. Brussels: NATO Standardization Office.
23. *NATO Glossary of Terms and Definitions AAP-06*. (2020). Brussels: NATO Standardization Office.
24. *North Atlantic Treaty Organization* (3 April 2025), https://www.nato.int/cps/en/natohq/topics_49755.htm, retrieved on 9 May 2025.

25. Naumescu, V. (4 February 2025). *Contributors*, <https://www.contributors.ro/europa-de-est-2025-intre-amenintarea-rusiei-iluziile-bine-intentionate-ale-ue-si-schimbarea-americii/>, retrieved on 9 May 2025.
26. Palavenis, D. (2025). “NATO enhanced forward presence in the Baltics: The nexus between the host and the framework nation”, in *Security and Defence* 49, no. 1.
27. Parlamentul României (2007). *Legea nr. 294 privind derularea în România a proiectelor finanțate prin Programul NATO de Investiții în Securitate*. București: Monitorul Oficial al României, no. 762.
28. Păvălașc, M. (24 November 2021). *Europa Liberă*, <https://romania.europalibera.org/a/tara-in-service-dunarea-potential-economic/32145121.html>, retrieved on 8 May 2025.
29. Pislaru, B. (22 April 2024). *Statistică INS: 49% din rețeaua publică este formată din drumuri modernizate*, <https://www.infofinanciar.ro/statistica-ins-reteaua-publica-drumuri-modernizate>, retrieved on 9 May 2025.
30. ROMATSA (w.y.), <https://www.romatsa.ro>, retrieved on 1 May 2025.
31. Santopinto, F. (2025). “The ReArm Europe Plan: Squaring the Circle Between Integration and National Sovereignty”. *French Institute for International and Strategic Affairs*.
32. SHAPE Public Affairs Office (1 July 2024). *NATO*, <https://shape.nato.int/news-archive/2024/stand-up-of-allied-reaction-force-marks-a-new-era-for-nato>, retrieved on 20 August 2025.
33. Umbrela Strategică (30 July 2025). *Umbrela Strategică*, https://umbrela-strategica.ro/romania-a-depus-la-ce-portofoliul-de-proiecte-pentru-programul-safe?utm_source=chatgpt.com, retrieved on 14 September 2025.

ADVANCING THE STRATEGIC RESILIENCE OF MILITARY MOBILITY THROUGH A WHOLE-OF-GOVERNMENT APPROACH

Associate Professor Dr. Maria CONSTANTINESCU

Regional Department for Defence Resources Management Studies, Braşov;

National Defence University “Carol I”, Bucharest

DOI: 10.55535/RMT.2025.3.32

This research paper explores the contribution military mobility can have to ensuring strategic resilience, by adopting a comprehensive, whole-of-government (WoG) perspective, emphasizing its critical role as a strategic capability for timely and effective deployment and sustainment of forces. It argues that military mobility transcends purely military functions and requires coordinated engagement among various government ministries – including defense, interior, and transportation – and collaboration with private sector stakeholders managing transport infrastructure. Challenges such as infrastructure degradation, lack of standardization in cross-border movement, and cybersecurity threats underscore the need for resilient, interoperable transport systems. The research underlines the imperative of embedding military mobility into national and multinational defense planning to ensure readiness, deterrence, and operational success in complex and evolving security environments.

Keywords: military mobility; whole-of-government approach; strategic resilience; hybrid threats; infrastructure vulnerability;

INTRODUCTION

Defined as the capacity for armed forces to swiftly and efficiently move personnel, materiel, and assets across diverse terrains and national borders (Damen, 2025), military mobility is a cornerstone of contemporary defense, rapid response, and the successful execution of military operations.

The *aim* of this paper is to analyze the contemporary challenges of military mobility in Romania and U and to make the case for the adoption of a whole-of-government framework. In order to achieve this aim, the following *research objectives* are considered:

- To analyze the complex challenges negatively impacting military mobility in Europe, encompassing both traditional obstacles such as inadequate physical infrastructure and regulatory complexities, as well as contemporary hybrid threats including cyberattacks, disinformation campaigns, and sabotage.
- To identify key requirements for effective military mobility within a whole-of-government paradigm, focusing on infrastructure development, regulatory harmonization, and strategies for mitigating hybrid threats.

Based on the analysis of the challenges to military mobility and the proposed benefits of an integrated approach, the following *research hypothesis* is formulated: The comprehensive adoption and effective implementation of a whole-of-government approach, encompassing coordinated efforts across governmental bodies, private sector entities, and international organizations, significantly enhances military mobility and strengthens resilience against hybrid threats in Europe.

This research will employ a *qualitative research methodology*, primarily utilizing content analysis and desk research to address the stated objectives. The primary *data sources* are derived from the academic literature review, official reports, and expert analysis.

LITERATURE REVIEW

There is a wide diversity in focus areas, methodological approaches, and geographic contexts in the literature that address multiple interconnected domains of military mobility, examining various aspects of strategic military mobility, resilience and whole-of-government approaches. Several foundational works examine

the strategic mobility framework, with early contributions (Drach, 1995) analyzing the four strategic mobility pillars of airlift, sealift, prepositioning, and infrastructure.

The need to integrate military mobility across various government sectors is addressed in the literature from different perspective. From the perspective of the organizational and technological integration, studies identify the need for seamless coordination between strategic and theater mobility systems (Kee, 1996), for aligning the force structure and mobility funding (Kokko, 1993) and for harmonizing the civil-military logistics doctrines (Gangotena-Bustamante, 2024). The role of artificial intelligence, predictive modeling, autonomous vehicles, and blockchain are highlighted as an important factors influencing military mobility in the future (Gangotena-Bustamante, *ib.*). In terms of policy recommendations, the examination of the literature suggested the need to consolidate command structures, develop multiservice knowledge-management organizations and encourage sustained knowledge acquisition and context-setting campaigns (Owen, 2017; Johnson, 2007). The human factors are considered a crucial component of resilient military mobility, with leadership, training, and professional development identified as essential for effective integration (Owen, 2013). While infrastructure gaps are visible, “soft” frictions (such as customs procedures, transport permits, and liability regimes) can impose equally significant delays. Recent analyses argue that these administrative hurdles, if unaddressed, could delay cross-border deployments by days or weeks, undermining the credibility of rapid reinforcement strategies (European Commission, 2022; Euractiv, 2024).

Military mobility cannot be effectively achieved without a resilient strategic infrastructure and reliable dual-use capabilities. Multiple studies (Drach, 1995) (Gardner, 1996) (Constantinescu, 2024) identify infrastructure – ports, airfields, roads, rail, and digital networks – as fundamental to force projection and sustainment. The vulnerability of these networks to physical, cyber, and hybrid threats is identified as a recurring concern, especially as military and civilian uses increasingly overlap (Chung et al., 2024), the authors emphasizing the need to update doctrines as to recognize infrastructure as a core component of mobility (Gardner, 1996), the crucial role of increased investments in dual-use (civil-military) transport corridors (Howell, 2020) and to adopt industry standards to ensure compatibility and resilience (Gardner, *ib.*). Some studies report that the integration of commercial assets, such as the Civil Reserve Air Fleet and the Voluntary Intermodal Sealift Agreement, is both a strength and a vulnerability, due to declining excess capacity and workforce shortages in the commercial sector (Gallagher, 2021).

The literature consistently identifies physical bottlenecks as critical vulnerabilities in terms of infrastructure and critical transport networks. Reports from the European Court of Auditors and the European Commission note that bridges unable to support heavy vehicles, rail networks with incompatible gauges, and ports lacking sufficient capacity all constrain rapid deployment (European Commission, 2022; European Court of Auditors, 2023). While EU transport initiatives have begun prioritizing dual-use infrastructure corridors, funding and timelines remain insufficient to match strategic requirements. This aligns with independent audits and journalistic reporting, which stress that despite significant policy attention, infrastructure upgrades continue to lag behind operational needs (Barigazzi, Herszenhorn, 2025).

The governance dimension has received particular emphasis in both academic and policy literature. Studies highlight that routine civil-military exercises are essential to overcoming institutional silos and building a shared culture of preparedness (Kraśniewski, 2023; NATO, 2023). However, barriers persist, as different agencies often operate with divergent risk tolerances, budgetary cycles, and regulatory regimes, producing friction at moments when speed and clarity are most critical (European Defence Agency, 2022). The mechanisms required for an effective WoG coordination in the domain of military mobility are addressed through several studies, which highlight the limitations of siloed approaches and advocate for integrated frameworks that leverage the capabilities of multiple government agencies, civilian sectors, and international partners. Some authors (Burton, 2007; Manwaring, 2006) recommend cross-governmental and multidimensional approaches, including modifications to command structures and the establishment of comprehensive policy coordination mechanisms, and others emphasize the role of civilian agencies and public-private partnerships in supporting military operations, particularly in logistics and infrastructure (Mars, 2016) (Jacuch, 2020) and in cyberspace (Myers, 2011; Constantinescu, 2025), underscoring the need for integrated governance and information-sharing across defense, transport.

Crisis response and preparedness are central to the strategic resilience of military mobility, and several studies (Ring, 2008; Wiltse, 2012) critique the lack of clear, coordinated military strategies for disaster response and advocate for total force solutions that integrate active, guard, and reserve components with civilian agencies, with emphasis placed on pre-event planning, intergovernmental relationships, and flexible response design for both domestic and international contingencies. The importance of civil preparedness and sector resilience is highlighted, particularly for rapid deployment across Europe and reinforcement of the North Atlantic Treaty Organization's Eastern Flank (Jacuch, 2020; Giurgiu et al.,

2024) and the development of dual-use infrastructure, simplification of cross-border procedures, and investment in logistics hubs are identified as practical strategies to enhance preparedness and responsiveness.

An emerging strand of literature explores the vulnerability of mobility to cyber and hybrid threats, with the conclusion that the resilience of military mobility must include cybersecurity, information integrity, and societal preparedness. This has reinforced calls for WoG cooperation between defence ministries, law enforcement agencies, and private operators of critical infrastructure (Giegerich, 2023; NATO, 2023).

CURRENT MILITARY MOBILITY CHALLENGES

The modern landscape of military operations is characterized by the continuing effects of legacy challenges (such as chronic underinvestment in dual use transport networks and legal obstacles), but also by increasingly complicated multifaceted threats that jeopardize the rapid and secure movement of forces and logistics.

Cyberattacks represent a pervasive and escalating threat to the infrastructure underpinning military mobility, targeting critical components such as transport sector infrastructure, energy grids, supply chains, and command-and-control systems and causing physical damage, or compromising sensitive data.

Over the past five years, cyberattacks on railway systems globally have increased, indicating a growing focus by malicious actors on disrupting rail operations. The European Union Agency for Cybersecurity (ENISA) has consistently reported on the evolving cyber risk profile of the transport sector, noting an increase in attacks against European transport infrastructure, including airports, ports, and railways. The agency emphasizes that ransomware and data-related threats are particularly prevalent, targeting IT systems that support various operational aspects of rail transport. The cross-border nature of cyber threats means that an attack in one country can have wider implications for interconnected European networks, affecting overall military mobility and logistical capabilities (ENISA, 2023). The vulnerabilities exploited often include IT systems related to passenger services, ticketing, and mobile applications, with ransomware being a primary threat vector, accounting for 45% of cyberattacks in the rail sector (Secureworld.io., 2024, Rail Journal, 2023).

In 2023, Poland experienced cyber intrusions in railway communication systems in 2023, causing emergency stops and delays, which highlighted the vulnerability of critical communication infrastructure (Cybersecurity and Infrastructure Security Agency, 2023). In 2025, Ukraine's state railway service experienced a powerful

cyberattack that disabled its online ticketing system, causing significant disruption, leading to long queues at stations as passengers were unable to purchase tickets online or via mobile applications (Reuters, 2025; The Record, 2025).

Cyberattacks are a major threat from a military mobility perspective, as they significantly impact the physical movement of military assets and personnel. Railway systems, being a cornerstone of military logistics for heavy equipment and large-scale troop movements, are particularly vulnerable. Attacks on operational technology (OT) systems, such as signaling, switching, and traffic control systems, can lead to widespread delays, rerouting, or even complete shutdowns of rail lines. A cyberattack that manipulates signaling systems could cause trains to halt, collide, or be misdirected, effectively creating bottlenecks and preventing timely deployment or redeployment of forces.

Cyberattacks can cripple the logistical planning and execution systems, with serious effects as modern military logistics rely heavily on sophisticated IT systems for inventory management, scheduling, route optimization, and supply chain coordination. A ransomware attack or data breach on these systems can render them inoperable, leading to a loss of situational awareness, inability to track assets, and severe delays in resupply efforts.

Cyberattacks are not solely aimed at disruption, they are increasingly used for intelligence gathering and surveillance, which indirectly impacts military mobility by compromising operational security. Adversaries can exploit vulnerabilities in transport networks to monitor the movement of military convoys, equipment, and personnel. By gaining access to scheduling systems, GPS data, or even public Wi-Fi networks used by military personnel, adversaries can infer troop movements, deployment patterns, and logistical vulnerabilities (Federal News Network, 2025).

Successful cyberattacks on critical infrastructure can erode public and military confidence in the security and reliability of transport systems, with significant psychological and operational consequences. Military commanders might become hesitant to rely on civilian infrastructure for critical movements, leading to slower, more cautious, and less efficient logistical planning. A loss of public trust can also lead to civil unrest or opposition to military movements, complicating operations that require civilian cooperation or access to public routes.

Responding to and recovering from cyberattacks on transport infrastructure can impose immense economic and resource strains, as the costs associated with system restoration, damage assessment, enhanced cybersecurity measures, and potential legal liabilities can divert significant funds and personnel away from other critical military priorities. Moreover, prolonged disruptions can lead to economic

losses for civilian industries, which in turn can impact the broader economic stability necessary to support military operations. The need to invest heavily in cybersecurity for civilian-owned infrastructure that underpins military mobility, such as rail networks, commercial ports, and airports, is a recognized challenge, with insufficient cybersecurity being a persistent issue (Industrial Cyber, 2025). Another issue which enhances the severity of the threat is that these cyberattacks usually target civilian and private companies, who may not have the will and/or resources to invest significantly in increasing their level of cybersecurity, making them softer targets compared for example with military logistic bases servers.

Disinformation campaigns may pose a significant threat to military mobility in Europe, especially in the context of heightened geopolitical tensions in Eastern Europe and the Baltic region, by undermining the integrity of strategic communications, destabilizing public trust, and complicating coordination among allied nations.

Disinformation campaigns often target the public and civil authorities to erode trust in military operations and government institutions, and false narratives about military build-ups, troop movements, or incidents involving infrastructure can lead to public unrest or opposition, thereby complicating command-and-control during crises. For example, a coordinated campaign on social media following the 2025 elections spread false reports claiming that Romania will send troops in Ukraine, with the result that even ordinary military convoys or planned military exercises were viewed with extreme suspicion by the population, considered as “*proof*” for that particular narrative (Inforadar, 2025). As a result of such disinformation campaigns, the movement of personnel and military material (NATO or national) on rail and roads may generate protests and in the event of a military operation, even lead to civil disobedience, distracting authorities and delaying mobilization.

Adversaries can use disinformation to distort or obscure real military developments, leading to confusion among decision-makers and false information about critical infrastructure damage or troop locations can mislead commanders, causing delays or misallocation of resources.

Disinformation campaigns can also falsely undermine the perception about transport infrastructure, influencing the movement of military logistics and supplies. For instance, rumors about unsafe rail routes or imminent attacks on key transport corridors might lead to unnecessary caution, rerouting, or closure of essential supply lines, or to crowding of essential military transport road routes by panicked civilians trying to flee certain areas.

In recent years, disinformation efforts targeting Europe have intensified, particularly surrounding the Russia-Ukraine conflict. For example, false claims about the destruction of key military infrastructure or false reports of troop withdrawals have periodically circulated, impacting strategic planning and public perception (European External Action Service, 2024). Similarly, manipulated satellite images and fake videos have been used to exaggerate or fabricate damage to critical transportation hubs, influencing decision-making and potentially delaying emergency or military responses.

Physical sabotage and covert actions inflict direct damage on infrastructure critical to military mobility, including roads, bridges, ports, and fuel supplies and can significantly impede logistical operations and rapid deployment capabilities. A specific characteristic of this type of hybrid warfare tool is the significant difficulty to demonstrate that a specific action was a deliberate sabotage, and to attribute it to a specific source/adversary. This feature makes this type of attacks particularly difficult to counter, as they may usually target civilian infrastructure and may mimic naturally occurring incidents. Malicious actors can leverage legal loopholes and online recruitment of third-country nationals to execute these operations, complicating attribution and accountability.

A widely publicized incident of this nature was the railway sabotage in Germany in 2022, when cables crucial for train communication and safety were intentionally damaged, leading to a significant disruption in rail services across northern Germany, isolating key military and civilian infrastructure. (Rinke, Marsh, 2022). In 2024 the railway bridge at Elsfleth-Orth in Germany suffered irreparable damage when it was struck by a barge, causing severe economic repercussions for the region's ports (Boote Magazin, 2025). This bridge is also crucial from a military mobility perspective, as it is part of the route connecting the port of Nordenham, Germany and Miesau, home to the Theater Logistics Support Center Europe's ammunition depot, a crucial NATO logistic facility. A temporary bridge became functional in April 2024, but was again struck by a tanker barge in July 2024 (Shipwrecklog, 2024). A recent report by the International Institute for Security Studies has identified a significant increase in such incidents in Europe following the 2022, from 2 events in 2018 and 2019 to 12 events in 2022, 9 events in 2023 and a peak of 33 events, distributed across all sectors – Water, Communications, Military, and Transport in 2024 (Edwards, Seidenstein, 2025).

Europe's transport *infrastructure limitations* are one of the main challenges to military mobility, as despite the fact that the continent is connected by an extensive transport infrastructure, this falls short of the requirements for rapid and large-scale

military movements. After the fall of the USSR, the transport sector has been almost exclusively considered as a civilian matter, leading to decades of underinvestment and a lack of focus on dual-use standards have left critical vulnerabilities.

Many European roads and bridges are not designed to withstand the weight and size of modern heavy military equipment, leading to significant delays and forced detours that directly impact the speed and efficiency of military deployments. These infrastructure limitations mean that moving military equipment and troops from Western Europe to the East can currently take weeks, and in some cases, months, a timeframe that is unacceptable for rapid response scenarios (Todd, 2025). A significant example comes from Germany, where 4,500 of its 40,000 bridges are in insufficient or deficient condition, rendering them incapable of handling heavy military vehicles (Hartmann, 2024).

The situation of the European rail networks also presents substantial challenges. A recent evaluation from Deutsche Bahn found that 23% of its 33,000 kilometers of track were in *“extremely bad condition”*, along with 48% of signaling control centers, 42% of level crossings, and over 25% of railroad switches, contributing to an average of one in three trains being delayed in 2022 (Hartmann, 2024). Another study concluded that, despite some progress and increased investments, the European rail system remains fragmented, with significant portions of the networks failing to fulfill the requirements set out in the EU’s core infrastructure policy, the Trans-European Transport Network (TEN-T). For instance, less than 20% of TEN-T corridors are equipped with the European Train Control System (ETCS) and the average speed of rail lines often remains low, with eight member states achieving a maximum speed of only 80 km/h on the majority of their lines, far below the goal of 160 km/h for the TEN-T (Rico, Heyl, 2025).

Inland waterways, including canals and rivers, also play a role in military logistics, but their aging infrastructure poses challenges. Locks and weirs are on average 65 years old, leading to frequent component failures and the closure of entire waterway sections, often without alternative routes. (Hartmann, 2024).

The resilience of military mobility in Europe is also challenged by bureaucratic hurdles and fragmented national regulations, which significantly affect the timely movement of military forces across European borders. A report by the European Court of Auditors (European Court of Auditors, 2025) has identified the problems generated by extensive red tape from fragmented procedures and a lack of coordinated effort at the EU level, as military equipment often faces restrictions at national borders due to exceeding local weight limits or encountering infrastructure (like bridges) not designed for heavy loads. Another hurdle is related to the slow

progress on “*Military Schengen*” as the EU’s first Military Mobility Action Plan (2018) experienced delays, and despite a subsequent plan (2021) allocating 1.69 billion euros to this purpose, there is still a significant funding gap. A final issue identified is the persistent lack of cohesive cross-border investment, as nations tend to neglect infrastructure along their borders, often viewing it as a neighbor’s responsibility. A significant challenge is also the absence of centralized coordination and effective information sharing mechanisms among EU member states, generating inefficiencies in planning and executing military movements and makes it difficult to implement military mobility plans in a targeted manner (Van Rensbergen, 2025).

Another area that needs to be considered in the efforts to increase the resilience of military mobility is the way the domain is going to be impacted by *emerging technologies*, such as artificial intelligence (AI), drones, and autonomous systems, which are increasingly being leveraged by adversaries and can disrupt traditional logistical and operational models. The conflict in Ukraine since 2022 has generated numerous lessons regarding the profound impact of drones not only on ground combat operations, but also through direct attacks on logistical convoys and supply routes (Hollenbeck, 2025) and through the use of low-cost sea drones to effectively challenge naval operations as seen with the Russian Black Sea fleet (Navy Lookout, 2025), opening the way for their use against naval transport. This widespread use of drones by adversaries can create a highly contested logistical space, forcing military movements to adapt to constant surveillance and potential interdiction, thereby slowing down deployments and increasing risks to personnel and equipment.

The integration of AI and autonomous systems by adversaries can introduce new layers of complexity and vulnerability to military mobility. While militaries are exploring AI for optimizing their own logistics and supply chain management, adversaries can exploit these technologies for disruptive purposes. For example, AI-enhanced intelligence can be used to analyze enemy doctrines and forecast responses, allowing for more precise targeting of logistical nodes and movement corridors. The threat of “*data poisoning*” could also compromise the integrity of AI-driven logistical planning and decision-making, leading to inefficiencies or misallocations of resources. Autonomous ground vehicles, while beneficial for reducing risk in high-danger operations, also present a new vector for attack if compromised or countered by adversary autonomous systems, potentially disrupting critical resupply efforts and creating chokepoints in military mobility (Lopez, 2024). Advancements in fields like quantum technology hold the potential to break asymmetric encryption and enable navigation systems that are resilient to GPS disruption, further complicating military mobility and logistics by challenging existing technological advantages (Kirichenko, 2025).

Electromagnetic warfare (EW) is another factor to be seriously considered in building resilience, as it directly targets critical communication and navigation systems, posing a significant threat to military mobility. A primary vulnerability lies in the Global Positioning System (GPS), which is highly susceptible to jamming and spoofing, potentially disorienting forces and disrupting logistical convoys. EW is already used by both parties in Ukraine, impacting both military and civilian GPS-dependent systems (Turgeon, 2024). A recent incident of this type has highlighted this risk, when the navigation system of a plane carrying Ursula von der Leyen to Bulgaria was disrupted due to suspected Russian interference, with the pilots having to land the plane using paper maps. (Davies, Vernon, 2025). EW can also involve electronic masking, probing, and reconnaissance, providing adversaries with critical intelligence on military movements and intentions, allowing for more effective targeting of logistical chokepoints or vulnerable convoys (NATO, 2023).

CONCLUSIONS AND RECOMMENDATIONS

The findings confirm the research hypothesis that the comprehensive adoption and effective implementation of a Whole-of-Government (WoG) approach is indispensable for significantly enhancing military mobility and strengthening resilience against these evolving threats. A WoG framework necessitates coordinated engagement across diverse governmental ministries – including defense, interior, transportation, foreign affairs, and finance – as well as robust collaboration with private sector stakeholders who manage critical transport infrastructure. This integrated strategy moves beyond siloed departmental efforts, recognizing that the resilience of military mobility is intrinsically linked to civilian preparedness, harmonized regulatory environments, and a shared understanding of security imperatives across society. The paper highlights that successful military mobility hinges on high-level political and military engagement, effective planning that seamlessly integrates civilian and military logistics, and the consistent application of WoG frameworks across enabling nations. Ultimately, advancing military mobility through a WoG approach is paramount for ensuring readiness, bolstering deterrence, and achieving operational success in an increasingly complex and unpredictable global security environment.

BIBLIOGRAPHICAL RESOURCES:

1. Barigazzi, J., Herszenhorn, D.M. (2025). *EU military mobility plan hampered by delays, lack of funding*. Politico, <https://www.politico.eu>, retrieved on 2 August 2025.
2. Boote Magazin (2025). *Millions in damages, Captain on trial after bridge crash*, <https://www.boote-magazin.de/en/travel-and-charter/territories/millions-in-damages-captain-on-trial-after-bridge-crash/>, retrieved on 12 August 2025.

3. Burton, A. (2007). *Developing a Whole-of-Government Approach to Complex Problems*.
4. Chung, S., Sardak, D., Cegan, J., Linkov, I. (2024). *Assessing the Robustness and Resilience of U.S. Strategic Highways: A Network Science Perspective*.
5. Constantinescu, M. (2025). *Building Resilience against Cybersecurity Risks in Military Transportation Networks*. International conference Knowledge-Based Organization.
6. Council of the European Union (2022). *Conclusions on military mobility*. Brussels: General Secretariat of the Council.
7. *Cyber hackers target Polish rail network, cause operational disruptions*, <https://industrialcyber.co/transport/cyber-hackers-target-polish-rail-network-cause-operational-disruptions/>, retrieved on 22 August 2025.
8. Damen, H. (2025). *Logistics and Mobility: The Backbone of Military Success*. Insparcom, <https://insparcom.nl/logistics-and-mobility-the-backbone-of-military-success>, retrieved on 2 August 2025.
9. Davies, M, Vernon, W. (2025). *EU chief von der Leyen's plane hit by suspected Russian GPS jamming*. BBC news, <https://www.bbc.com/news/articles/c9d07z1439zo>, retrieved on 22 August 2025.
10. Drach, A. 1995. *The Strategic Mobility Shortfall: Underrepresented, Underfunded, and Unresolved*.
11. Edwards, C., Seidenstein, N. (2025). *The Scale of Russian Sabotage Operations against Europe's Critical Infrastructure*, The International Institute for Strategic Studies.
12. *ENISA Threat Landscape: transport sector*, <https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape>, retrieved on 2 August 2025.
13. Euractiv (10 March 2024). *EU struggles with military transport bureaucracy despite action plan*, <https://www.euractiv.com>, retrieved on 22 August 2025.
14. European Commission (2022). *Action Plan on Military Mobility 2.0* (JOIN(2022) 49 final). Brussels: European Commission.
15. European Commission (2025), https://transport.ec.europa.eu/news-events/news/commission-supports-military-mobility-projects-eu807-million-2024-01-24_en, retrieved on 22 August 2025.
16. European Commission. *Military mobility*, https://transport.ec.europa.eu/transport-themes/military-mobility_en, retrieved on 22 August 2025.
17. European Court of Auditors (2023). *Special Report: The EU's action on military mobility – Slow progress in removing obstacles*. Luxembourg: Publications Office of the European Union.
18. European Court of Auditors (2025). *EU military mobility – Full speed not reached due to design weaknesses and obstacles en route*, https://www.eca.europa.eu/ECAPublications/SR-2025-04/SR-2025-04_EN.pdf, retrieved on 2 August 2025.
19. European Defence Agency (2022). *Defence implications of a whole-of-government approach*. Brussels: EDA.
20. European External Action Service (2024). *Disinformation and Strategic Deception in the Ukraine War*, <https://eeas.europa.eu/>, retrieved on 2 August 2025.
21. Federal News Network (19 August 2025). *Weaponized infrastructure: The overlooked digital threat to US forces*, <https://federalnewsnetwork.com/commentary/2025/08/weaponized-infrastructure-the-overlooked-digital-threat-to-us-forces/>, retrieved on 22 August 2025.

22. Gallagher, R.E., Burch, G.F., Batchelor, J.H. (2021). *United States Civil Reserve Air Fleet (CRAF): A Brief History – Formation, Functionality, and Future*. Transportation Research Record.
23. Gangotena-Bustamante, J.B. (2024). *Diseño de sistemas logísticos resilientes para fuerzas desplegadas en regiones inestables*, in *Space Scientific Journal of Multidisciplinary*.
24. Gardner, G. (1996). *Infrastructure, the Fourth Element of Strategic Mobility*.
25. Giegerich, B. (2023). *Cyber and hybrid threats to mobility and logistics in Europe*, in *Survival*, 65(4), pp. 121-140.
26. Giurgiu, T., Virca, I., Noja, G. (2024). *Military Mobility in the Vision of NATO and European Union*, in *Romanian Military Thinking*.
27. Hartmann, J. (2024). *Military Mobility*. DGAP, <https://dgap.org/en/research/publications/military-mobility>, retrieved on 22 August 2025.
28. Hollenbeck, N. (2025). *How to Transform the Army for Drone Warfare*. Army War College, <https://warroom.armywarcollege.edu/articles/transform-for-drones/>, retrieved on 2 August 2025.
29. Howell, R. (2020). *Transportation Infrastructure: A Critical Component for Deterrence in Europe*, U.S. Army Command and General Staff College, <https://apps.dtic.mil/sti/pdfs/AD1159121.pdf>, retrieved on 18 January 2024 (In-text citation Howell, 2020).
30. Industrial Cyber (2025). *Cyber threats to rail, ports and airports could cripple US military mobilization*, FDD report warns.
31. Inforadar, *Dezinformare pe tema sprijinului pentru Ucraina*, https://inforadar.mapn.ro/tema/104_dezinformare-pe-tema-sprijinului-pentru-ucraina, retrieved on 2 August 2025.
32. Jacuch, A. (2020). *Security and defense challenges – civil preparedness in NATO*.
33. Johnston, M. (1996). *Strategic Mobility: An Assessment*, <https://apps.dtic.mil/sti/html/tr/ADA308551/index.html>, retrieved on 2 August 2025.
34. Kee, R.A. (1996). *Bridging the Gulf between Theater and Strategic Air Mobility*.
35. Kirichenko, D. (2025). *Artificial intelligence's growing role in modern warfare*. Army War College, <https://warroom.armywarcollege.edu/articles/ais-growing-role/>, retrieved on 2 August 2025.
36. Kokko, R.W. (1993). *Strategic Mobility for the National Military Strategy*.
37. Kraśniewski, P. (2023). *Interagency coordination for defence logistics: A whole-of-government challenge*. *Security & Defence Quarterly*, 42(3), pp. 33-47.
38. Lopez, T. (2024). *DOD Needs Solutions for the Proliferation of Autonomous Vehicles, Defense Officials Say*. Defense Logistic Agency, <https://www.dla.mil/About-DLA/News/News-Article-View/Article/3869110/dod-needs-solutions-for-the-proliferation-of-autonomous-vehicles-defense-offici/>, retrieved on 2 August 2025.
39. Manwaring, M. 2006. *Defense, Development, and Diplomacy (3D): Canadian and U.S. Military Perspectives*.
40. Mars, H. (2016). *How the Department of Transportation Supports the DOD*.
41. NATO (2023). *Electromagnetic warfare*, https://www.nato.int/cps/en/natohq/topics_80906.htm, retrieved on 2 August 2025.
42. NATO (2023). *Resilience and civil preparedness*. Brussels: NATO Headquarters, <https://www.nato.int>, retrieved on 2 August 2025.

43. Navy Lookout (2025). *Black Sea battle: how Ukraine's drones overpowered the Russian Navy*, <https://www.navylookout.com/black-sea-battle-how-ukraines-drones-overpowered-the-russian-navy/>, retrieved on 2 August 2025.
44. Owen (2017). *US Air Force Airlift and the Army's Relevance*. Parameters
45. Rail Journal (22 March 2023). *EU cybersecurity agency reports on threat to rail*, <https://www.railjournal.com/technology/eu-cybersecurity-agency-reports-on-threat-to-rail/>, retrieved on 2 August 2025.
46. Reuters (24 March 2025). *Ukraine sees Russian effort to sow chaos as cyberattack hits railway online systems*, <https://www.reuters.com/world/europe/ukraine-railway-says-its-online-systems-targeted-large-scale-cyberattack-2025-03-24/>, retrieved on 2 August 2025.
47. Rico, C., Heyl, B. (2025). *Transport & Environment. The State of the EU's Rail Infrastructure: Investment priorities for more connected and resilient networks*, <https://www.transportenvironment.org/articles/the-state-of-the-eus-rail-infrastructure>, retrieved on 2 August 2025.
48. Ring, K. (2008). *Military Disaster Response: Strategy, Leadership, and Actions-Closing the Gap*.
49. Rinke, A., Marsh, S. *Malicious and targeted sabotage halts rail traffic in northern Germany*, <https://www.reuters.com/world/europe/rail-northern-germany-standstill-due-technical-issue-2022-10-08/>, retrieved on 2 August 2025.
50. Secureworld.io. (20 August 2024). *Cyber Attacks on Railway Systems Increase by 220%*, <https://www.secureworld.io/industry-news/railway-cyber-attacks>, retrieved on 2 August 2025.
51. The Record (24 March 2025). *Cyberattack hits Ukrainian state railway, disrupting online ticket system*, <https://therecord.media/ukraine-railway-ukrзалізnyticia-cyberattack-online-ticket-system>, retrieved on 2 August 2025.
52. Todd, S. (16 September 2025). *EU Military Mobility Package addresses long-standing weaknesses in Europe's transport networks*, <https://www.ajot.com/premium/ajot-eu-military-mobility-package-addresses-long-standing-weaknesses-in-europes-transport-networks>, retrieved on 2 August 2025.
53. Turgeon, T. (2024). *GPS Spoofing at Russia's Borders: What to Know. GNSS jamming*, <https://www.gnssjamming.com/post/gps-spoofing-report-october-2024>, retrieved on 2 August 2025.
54. Van Rensbergen, A. (2025). *Red tape and underfunding slow down EU 'military Schengen'*. The Parliament Magazine, <https://www.theparliamentmagazine.eu/news/article/bureaucracy-and-underfunding-undermine-eu-military-mobility>, retrieved on 2 August 2025.
55. Wiltse, J. (2012). *Before the Next Hurricane Katrina: A Strategic Approach to Enhancing Military Capabilities*.
56. <https://shipwrecklog.com/log/tag/elsfleth-bridge/>, retrieved on 2 August 2025.
57. <https://www.iiss.org/research-paper/2025/08/the-scale-of-russian--sabotage-operations--against-europes-critical--infrastructure/>, retrieved on 2 August 2025.

EDUCATIONAL BOOTCAMP FOR THE VOCATIONAL DEVELOPMENT OF ADOLESCENTS IN RESILIENT SOCIETIES – A PROPOSAL BASED ON PROJECT MANAGEMENT –

Colonel Professor Dr. Dorel BADEA, BEng

Associate Professor Dr. Diana Elena RANF

Assistant Professor Dr. Elisabeta-Emilia HALMAGHI

“Nicolae Bălcescu” Land Forces Academy, Sibiu

DOI: 10.55535/RMT.2025.3.33

The article presents the main lines of effort for implementing an extracurricular program dedicated to the development of adolescents in national vocational high schools with a military profile.

The proposed framework is subsumed under the imperatives of STEAM education, tailored to the military field, based on a project management approach, with an appropriate quantitative and qualitative methodology.

The study highlights the premise that the target audience is a valuable resource for training active officers, military quartermasters, and non-commissioned officers.

Keywords: development; resources; vocation; project; defence;

THE GENERAL, CONCEPTUAL, AND PRACTICAL FRAMEWORK OF THE APPROACH

Transforming current educational systems is an essential action in today's world, with the ultimate goal of producing teenagers who are highly adaptable to future challenges in a volatile, uncertain, complex, and ambiguous environment. The issue at stake, linked to the irreversible trend of processes specific to digitalisation, Industry 4.0 and artificial intelligence, requires a public agenda focused on the *development of adolescents* (vocational education, military profile) adapted to these interdisciplinary realities. In this context, it is essential to provide the target group with viable solutions for cultivating resilient behaviour through which they can understand current socio-technical mechanisms and develop harmoniously as future professionals and citizens. The direct beneficiaries of the project-based approach are 11th grade students at a National Military College (NMC). Using STEAM (*Science, Technology, Engineering, Arts and Maths*) solutions, a modern learning experience (in the form of lectures and summer school activities) is proposed, which will bring short-term added value in terms of adapting learning to the stage of training for the transition to university education. The deliverables offered increase young people's interest in the practical side of STEAM, mainly through the use of collaborative working models, critical thinking, teamwork, simulation, gamification, and experience transfer.

The quality of training for this category of human resources is essential for the process of generating human resources for security and defence, given that military college graduates constitute the main component of admissions to military educational institutions for the training of future officers, military quartermasters, and non-commissioned officers. Given the current requirements, a high level of STEAM knowledge is needed, taking into account the contemporary realities of war.

The idea of a resilient society was chosen for the title because, at present, the concept encompasses both challenges and, complementarily, opportunities, due to its complexity and implications for military organization management in general and defence human resources management in particular. An example of existing international concerns in terms of strengthening the framework outlined above is provided by the idea of the CORE project (European Commission, CORDIS – Eu results, sScience and human factOr for Resilient sociEty). The fact that knowledge specific

to STEAM education (with clearly defined learning outcomes) is implemented in initial military vocational training facilitates, at the university level, the understanding of advanced concepts applied in practice at the level of integrated technical systems platforms and the acquisition of skills appropriate to the military profession. In other words, the fact that future students have a much more solid general and specialized knowledge base allows them to better understand the changes occurring in the field and to adapt much better (quantitatively and qualitatively) to the new changes, i.e., to be more resilient.

Such a formative approach requires a solid technique, correctly applied to the general specifics of military education (Magnussen, Boe, Torgersen, 2023) and the military organization (Iancu, 2022) itself, which led to the consideration of project management as an implementation solution. Regarding the specifics, necessity, and practical usefulness of project management, it is stated that the appropriateness or even difficulty of success is such that: *“The appropriateness of a project may be a matter of taste, nuance, or perspective. Of course, assessing the viability of a project also involves a degree of subjectivity, which is inherent in any human judgment or, in any case, difficult to avoid.”* (Vladu, Pîrvan, 2024, p. 24.)

DESCRIPTION OF THE PROPOSED SOLUTION

The main focus of the project team (10 people, teaching and research staff) is on achieving the project objectives. The collaborative workspace and activities supporting the achievement of five objectives have been defined in three dimensions by: (a) the technical, systemic, and operational perspectives of the STEAM field; (b) institutional missions, rule enforcement, and resource allocation as the main types of organizational processes targeted; (c) source, sensor, and decision-maker, as qualities of the stakeholders involved. Upon completion of the project, from an educational point of view, it is imperative to ensure the fulfilment of the goal of harmonizing the triad formed by *cognitive involvement* (specific to the age of the adolescents considered the target group), *understanding the general concepts* used in the field of resilience and social security (facilitated by the specificity of STEAM), and, last but not least, *increasing interest in knowledge* (through teaching strategies that facilitate the attractiveness of science).

The objectives designed to be achieved through the application proposed by the project team are:

- **O1.** Supporting the transformation of Romanian pre-university education by involving high school students, vocational stream, military profile, in interdisciplinary learning experiences, in a STEAM context, appropriate to the requirements of a constantly changing society;

- **02.** Raising awareness among military high school students of the contribution of STEAM subjects to the development of transversal skills, such as critical thinking and creativity, in the development of innovative solutions that respond to the complexity of contemporary problems;
- **03.** Increasing the motivation of young adolescents for school, for multilateral development, stimulated by the identification of current development opportunities;
- **04.** Developing and internalizing personal values that enable them, as citizens and professionals in training, to respond appropriately, confidently, and resiliently to technical changes that impact society;
- **05.** Encouraging the exchange of experiences between generations, based on self-knowledge and knowledge, in real and simulated situations, dominated by current scientific and technological paradigms.

The topic contains the deliverables and objectives detailed below.

Deliverable 1 – Project launch event

1.1 Project launch conference. A presentation will be made on the project's objectives, stages/phases, and expected outcomes, highlighting the project's context and targeted results. The aim is to raise awareness among adolescents at this stage about the challenges of today's society and the need to train and develop themselves in order to respond to these challenges as effectively as possible, both in terms of vocational maturation and training as responsible adolescents in relation to their role as citizens and professionals in the field of security and defence.

Deliverable 2 – Lecture series

2.1 Critical thinking in research, development, and innovation for a resilient society. The lecture aims to raise awareness among teenagers of the need to develop critical thinking in order to achieve the goal of building a safe and resilient society. The theme will focus on the development of skills, attitudes, and habits specific to the manifestation of critical thinking in the context of contemporary society. The place and role of citizens in today's and tomorrow's society will be analysed, as well as ways of using appropriate algorithms to interpret processes in the environment. Emphasis will be placed on presenting the possibilities of using science to identify logical and realistic solutions for strengthening individual and social resilience.

2.2 Collaborative responsibility in sustainability and entrepreneurship. The theme aims to develop cross-cutting skills among adolescents that facilitate innovation. Starting from the argument that entrepreneurship is important at the societal level, the lecture focuses on describing the concept, presenting its evolution at the global and national levels, and highlighting examples of how entrepreneurship can respond to a problem or opportunity. The theme connects entrepreneurship

with sustainability to explain to young people that entrepreneurs must be responsible and that innovation must be sustainable, respecting the principles of non-discrimination and equal opportunities. Another objective of this lecture is to highlight the collaborative aspect of innovation and change. The phenomenon of entrepreneurship has gained momentum, facilitated by the current legislative framework, scientific and technological progress, existing financing opportunities, but especially due to the involvement of the academic environment as a partner in dialogue and a framework for disseminating information to stakeholders, public or private actors.

2.3 Modern technologies at the service of society: current applicability, development opportunities, and security challenges. This topic aims to create a framework that is easy to understand and adapted to the level of preparation of the target group (17-year-olds) in order to improve their perception of trends in the development of contemporary technologies. The aim is to understand their usefulness and the concrete advantages they bring to the functionality of various areas of everyday life, while at the same time providing a balanced overview of their vulnerability and associated risks. A special subchapter is devoted to digital technologies and how STEAM impacts social development. It also addresses the main trends in technological development at NATO level, in the dual-use sector and for civil emergency management.

2.4 The multidimensionality of security culture – between technical imperatives and the need for human development. The lecture aims to help young people become aware of the need to develop a robust security culture by combining technology with human development in order to instil in them a sense of responsibility for individual protection and collective safety. The theme will address the dimensions of security culture in interdependence with the human and technological factors, thereby contributing to the development of the skills so necessary for the younger generation to face the challenges of an increasingly complex world, helping them to become not only responsible users of technology, but also involved and resilient citizens.

Deliverable 3 – Selection based on a project competition

3.1 Establishing the competition information package. The transition from deliverable 2 to deliverable 4, in terms of target group selection (from 120 to 25 people), will be made following the competition between the two deliverables, based on the preparation of a project entitled: *Solutions based on modern technologies for a resilient society*. The conditions for participation, evaluation criteria, project implementation criteria, and deadlines will be included in an information package

that will be brought to the attention of the target group, both upon completion of deliverable 2 and through the specific section of the project created separately on the website https://www.armyacademy.ro/managementul_proiecte_cercetare.php

3.2 Monitoring of the competition. Following the submission of applications on a MOODLE-type IT platform, with a link that will be communicated to beneficiaries, the project submission stage will be monitored according to the schedule established and communicated to participants, and administrative assistance will be provided as appropriate.

3.3 Evaluation and selection. *After the deadline for submitting projects, each project proposal will be evaluated by a panel of three evaluators from within the project.* The project manager will determine the composition of the three evaluation panels and assign the projects for evaluation. Following the ranking of the scores obtained, the first 25 applications in descending order of score will be declared winners for participation in the summer school. The results of the selection process will be communicated to the beneficiaries via the MOODLE IT platform and will also be published on the project's dedicated page.

Deliverable 4 – Summer School

4.1 The evolution of techniques and technologies. Case study for Romania: from folk techniques to startups dedicated to digital technologies. A thematic workshop will be organized at the ASTRA Museum of Traditional Folk Civilization in Sibiu, which provides an authentic setting for exploring the transition from folk techniques to modern technologies. The workshop will focus on: exploring Romanian techniques and technologies and presenting how folk techniques (crafts, traditional tools, indigenous devices, etc.) have influenced the development of modern technological solutions; presenting case studies of local innovation, based on Romanian startups that have transformed creative ideas into competitive digital technological solutions, highlighting the development process from concept to implementation; participation in an interactive innovation workshop, based on a practical session in which young people create a digital prototype inspired by traditional Romanian techniques and physically produce it using modern technologies (such as 3D printing); participation in a brainstorming activity in which participants are actively involved in identifying solutions for promoting and/or improving the heritage exhibited in the museum, based on digital technologies (Internet of Things, holograms, VR/AR technologies, etc.).

4.2 Features of military techniques and technologies. Case study: dual-use technologies. The evolution, role, characteristics, and operational usefulness of current military techniques and technologies will be presented. The aim is to conduct presentations and demonstrations of dual-use equipment available in the host institution's laboratories. The focus of this topic will be on interactive, hands-

on activities involving the use of dual-use technologies, such as mini-drones, mini-robots, VR/AR glasses, and 3D printing, available at „Nicolae Bălcescu” Land Forces Academy of Sibiu (NBLFA). A role-playing session will be held to discuss aspects related to the industry’s interest in military technology.

4.3 Technical solutions for modelling and simulating activities in the field of security. The activity aims to familiarize teenagers with serious gaming solutions used for education. The transition from reality (through simplification, essentialisation, abstraction) to model (including mathematical models) will be explained. Specifically, participants will be familiarised with the Virtual Battlespace (VBS3) virtual training system and will take part in an airsoft activity. The aim is to raise awareness among teenagers about the role of simulations in the field of security and civil emergencies and, in particular, to highlight the importance of STEAM in the transition from reality to conceptual models that can be used in simulation, for a robust transfer of experience. The necessary infrastructure is available at NBLFA, within the Military Action Modelling and Simulation Centre (through Military Action Modelling and Simulation Laboratories 1 and 2, the Robotics and Artificial Intelligence Laboratory and the MILES and Drones Department). Complementarily, the aim is to understand the evolution of modelling and simulation, correlated with the evolution of techniques and technologies at NATO and EU level.

4.4 Sustainable approaches for a sustainable society. The activity aims to identify creative and innovative solutions for a sustainable society. Starting from an integrated approach to STEAM education and education for sustainability, participants will work in teams and be encouraged to use both scientific and technical knowledge and skills such as critical thinking, systemic thinking, problem solving, and decision making to develop solutions to current challenges. In addition to developing technical, scientific, and entrepreneurial skills, the activity also aims to raise awareness of environmental and social responsibility and promote sustainability values through experimentation, problem-solving, and teamwork.

4.5 From misinformation in the digital age to hygiene for cyber resilience. The aim of the activity is to develop critical thinking in young people and to train them in practical skills in the field of social engineering related to the use of technology in everyday life, so that they become more responsible and resilient to online manipulation and attacks. The activity is designed to help young people understand how to recognize and avoid cyber traps and risks in the digital age. The activity combines two essential themes for the modern world: accurate information and digital safety, in a way that is engaging and relevant to the younger generation.

Deliverable 5 – Project closing event

5.1 Project closing conference. The results obtained within the project will be presented, final feedback from the beneficiary will be provided, and the

sustainability requirements of the project will be highlighted. The information resource package will be presented and distributed to both the participants of the selected NMC and all national military colleges.

Considering the proposed objectives and the topics of the planned deliverables, the relevance of organizing and carrying out the activities, divided into three main categories of deliverables, is presented in detail below.

A. For the deliverable *Lecture Series*, held at the NMC headquarters and scheduled to take place in May, a series of four lectures was envisaged, with topical subjects related to the current state of development of the STEAM field, the way in which military high school education is carried out in Romania in the vocational stream, the military profile and, last but not least, related to current societal challenges in terms of security and resilience. The proposed topics are relevant for raising awareness of the challenges, implicitly with specific educational imperatives, in areas such as *Culture, creativity, and inclusive society* (with an impact on social and economic resilience) and *Civil security for society* (with an impact on the sector of cybersecurity growth), as set out in national strategic documents on research, innovation, and smart specialization. The training of responsible citizens, especially for the vocational stream, begins in high school, and the provision of educational programs that integrate current trends in science is an added bonus in generating an educational profile adapted to the current and future requirements of society. The unprecedented development of technology and techniques brings with it advantages and disadvantages, the latter having the potential to turn into vulnerabilities or even threats, with widespread societal effects. We want to raise awareness among the target group that we are all part of the possible solutions to be developed in the aforementioned context, and that science, approached in an interdisciplinary and transdisciplinary manner, plays an overwhelming role in shaping the mindset appropriate to these realities. Problem-solving, critical thinking, and discovering new perspectives on the proposed topics are relevant in the context of transforming adolescents to a higher level of maturity in the exercise of knowledge.

B. The deliverable *Selection based on a project competition* (scheduled to take place in July) aims to select 25 students from the initial target group to participate in the summer school organized at NBLFA. The aim is to assess the students' potential to understand the role of modern technologies in serving society (in order to create greater resilience) and to encourage creative behaviour in proposing solutions on a given topic. Attitudinally, but also practically, this stage aims to correctly assess the need to ensure a balance between rigor (by complying with the specifications of the project-specific information package) and flexibility (through the scalability

of the proposed solution and the way a STEAM application is replicated in the final solution). This increases self-esteem, responsibility, and confidence in the level of maturity achieved. The ability to use project-based management is developed, with the design of solutions to societal problems, and, subsumed, awareness of the role of universal constraints (time, quality, resources, skills) and planning (as an essential function of management).

C. For the deliverable called *Summer School*, scheduled to take place in August, the aim is to continue the themes from the lecture session, resulting in five practical and applied activities. The goal here is to improve technical skills in the field of technology in general, and in the cyber-digital area in particular. Since certain activities will involve teamwork, there is an emphasis on collaborative skills, with participants being encouraged to step outside their comfort zone in terms of ideas and actions. They are thus involved in brainstorming sessions and red flag exercises that demonstrate the importance of group cohesion, which is less successful in formal activities. The aim is to raise awareness of the socio-technical multidimensionality of security culture and, by extension, the role of STEAM in providing education tailored to the needs of diverse socio-professional categories.

For the lectures, the target group consists of 120 11th grade students, who at the end of the project will be in 12th grade and will be preparing for admission to higher military education institutions. For the *Summer School* deliverable, scheduled for the end of August, before the start of the school year, 25 students will be selected on the basis of a project competition. The projected impact consists of:

- informing and stimulating beneficiaries' interest in STEAM subjects by combining formal education with non-formal education;
- developing skills among young people, such as technical skills, communication and teamwork, critical thinking, problem solving, and competitiveness, by involving them in interactive summer school activities and in the competition to select participants for activities;
- stimulating the creative and innovative side of students by helping them acquire entrepreneurial skills and motivating them to get involved in developing sustainable solutions adapted to contemporary realities;
- increasing motivation for learning and performance by integrating into the activities carried out, specific to the three deliverables (2-4), new learning strategies facilitated by access to new technologies (artificial intelligence), which allow the development of transversal and digital skills.

The outcome indicators for the planned deliverables are presented in *Table 1*.

Table 1: The outcome indicators for the planned deliverables
(authors' conception)

Nr. indicator	Projected result indicators	Unit of measurement	Assumed value
1	Number of lectures given	Number	4
2	Number of students participating in the lecture series	Number	120
3	Project selection competition for participation in the <i>Summer School</i>	Number	1
4	Applications submitted for participation in the <i>Summer School</i>	Number	40
5	Applications accepted for participation in the <i>Summer School</i>	Number	25
6	Number of practical activities carried out during the Summer School	Number	5
7	Number of participants in the Summer School	Number	25
8	Percentage of <i>Summer School</i> participants who consider (via feedback questionnaire) that they have acquired new skills or practical tools to address security and resilience issues	Percentage	75
9	Percentage of total participants who consider (via feedback questionnaire) that they have acquired new skills or useful knowledge	Percentage	75
10	Post-event questionnaires	Number	2
11	Dissemination of results - good practice reports	Number	1
12	Dissemination of results - scientific articles in BDI journals	Number	2

The indirect beneficiaries (which supports the national character of the project) are students from the other four military high schools in the country. They will each receive an information package containing the resources developed during the project, the content of which will be presented during visits to promote the image of the institution (an activity that NBLFA carries out annually in national military

colleges) and during the visits that national military colleges make annually to military academies to provide information on the specifics of the officer profession (https://www.armyacademy.ro/ev_2024_09_25.php). In the case of national colleges and civilian high schools, the results obtained are disseminated through the project website and through visits that high schools make to the NBLFA headquarters during the *Alternative School program*, the *NBLFA Open Day*, and the *Romanian Army Day in Schools* (https://www.armyacademy.ro/ev_arhiva.php#octombrie2024). The expected impact on indirect beneficiaries consists of:

- documenting stakeholders on everything related to involvement in the implementation of STEAM programs and the benefits that can be obtained;
- the possibility of providing information on the changes that are expected and that result from the combination of science and innovation, as a result of the materials disseminated in military high schools and published on the project website;
- encouraging students to get involved in similar activities (carried out at the direct beneficiary) by increasing their motivation for personal development, knowledge exchange, and learning the latest scientific and technological concepts;
- raising awareness of the opportunity to access, through such initiatives, visits to laboratories and spaces equipped with the latest technologies, with the capacity to simulate complex processes and situations.

The estimated budget for the planned activities is presented in *Table 2*.

Table 2: Budget and categories of planned expenditures
(authors' conception)

TOTAL PROJECT	Categories of expenses	National budget (lei)	Own sources budget (lei)	Total (lei)
	1. <i>Personnel expenses</i> (including employer contributions)	140.000	0	140.000
	2. <i>Logistics expenses</i>	53.000	0	53.000
	2.1. Inventory expenses	24.600	0	24.600
	2.2. Expenses for services performed by third parties	28.400	0	28.400
	3. <i>Travel expenses</i>	50.000	0	50.000
	4. <i>Indirect expenses</i> (max. 5% of direct expenses)	7.000	0	7.000
	Total project (1 + 2 + 3 + 4)	250.000	0	250.000

CONCLUSIONS

The solution presented may be applicable to all national military colleges in Romania, but in this case, the triple constraint specific to project management is at a much higher level than the requirements. The costs of implementation increase and, of course, greater capacity is required from the implementation team and institution. The implementing institution leading the project can be any of the military academies in the national higher military education system.

The increase in the number of beneficiaries from a college, combined with the implementation of the project in all existing military colleges at the national level, leads to the opportunity to consider a program with the integration of stand-alone projects for each college. In this case, the involvement of all existing military academies at the national level can also be considered.

The implementation of an iteration, as presented, provides an adequate space for identifying lessons learned, thereby ensuring the scalability of the solution at the program management level, even in the context of a different subject and skills to be developed.

BIBLIOGRAPHY:

1. European Comission. CORDIS – EU results (2025). *Science and human factor for Resilient sociEty*, <https://cordis.europa.eu/project/id/101021746>, retrieved on 24 August 2025.
2. Iancu, D. (2022). *Managementul organizației militare: elemente fundamentale*. Sibiu: Editura Academiei Forțelor Terestre “Nicolae Bălcescu”.
3. Magnussen, L.I., Boe, O., Torgersen, G.-E. (2023). *Agon – Are Military Officers Educated for Modern Society?* Education Sciences, 13(5), 497, <https://doi.org/10.3390/educsci13050497>, retrieved on 24 August 2025.
4. Vladu, L., Pîrvan, M. (2024). *Management de proiect: cum transformăm o idee bună într-un rezultat durabil*. București: Editura Comunicare.ro.

RESILIENCE AMONG FUTURE MILITARY LEADERS – COMPARATIVE STUDY AMONG THE STUDENTS OF THE “NICOLAE BĂLCESCU” LAND FORCES ACADEMY –

Associate Professor Dr. Raluca RUSU

“Nicolae Bălcescu” Land Forces Academy, Sibiu

DOI: 10.55535/RMT.2025.3.34

In the context of the increasingly complex challenges of the military operational environment, developing resilience among future military leaders has become a strategic priority. Resilience enables leaders to cope with acute stress, uncertainty, and decision-making pressure. This paper highlights the essential role of resilience in maintaining performance, preventing burnout, and promoting ethical conduct in high-stakes situations. Considering this, we identified the level of resilience among military students at the “Nicolae Bălcescu” Land Forces Academy in Sibiu, from both the first and third years of study. The comparative analysis of the two groups allowed us to observe whether resilience increases during the course of military training. The study used the College Students’ Resilience Scale, composed of four dimensions: self-efficacy and adaptability, perception and use of social support, positive cognition, and the ability to adapt to negative emotions. The results indicate a higher general average recorded in the third year ($M = 3.18$), compared to the first year ($M = 2.86$). Overall, the results confirm not only an increase in self-efficacy, social support, and positive cognition, but also a significant strengthening of emotional resilience over time.

Keywords: resilience; self-efficacy and adaptability; perception and use of social support; positive cognition; ability to adapt;

INTRODUCTION

In the contemporary military environment, characterized by uncertainty, exposure to multiple risks, and constant psychological pressure, developing resilience has become essential for maintaining performance and mental health. For military leaders, this capacity is even more important, as they act not only as decision-makers in critical situations but also as sources of moral support and stability for subordinates. Resilience in military leadership has been associated with increased resistance to operational stress, stronger team cohesion, and reduced risk of psychological exhaustion. Moreover, resilience is not a passive trait but one that can be actively cultivated through psychological training programs, organizational support, and positive leadership – especially through formal education. In this sense, resilience is not just a personal quality but a strategic goal for modern armed forces that aim to develop leaders capable of managing pressure and acting ethically in complex situations.

WHAT IS RESILIENCE?

In the psychological community, resilience is a quality that allows an individual to recover from adversity stronger than before. The factors that make an individual psychologically resilient are often emotional and attitudinal; in this sense, *“the primary metric of resilience is the individual’s emotional well-being.”* (Zolli, Healy, 2012, p. 7).

Resilience is the psychological capacity of a person to effectively cope with adversity, intense stress, trauma, or significant changes, while maintaining or returning to an optimal level of functioning. In specialized literature, it is often described as a dynamic process of positive adaptation in the face of risk factors or external pressure (Demerouti et al., 2001). In the military context, resilience involves not only psychological survival under operational stress but also the ability to make effective decisions, maintain moral integrity, and lead responsibly even in extreme situations (Meredith et al., 2011).

Fletcher and Sarkar (2013), in their work *“Psychological Resilience: A Review and Critique of Definitions, Concepts, and Theory”*, review and critique the variety of definitions, concepts, and theories of resilience, emphasizing the need for rigorous

conceptual clarification. They identify two central concepts underlying most definitions of resilience: *adversity and positive adaptation*. Resilience involves both exposure to challenges and the ability to respond constructively and appropriately to the given context.

Building on this, the idea emerges that resilience is not a fixed characteristic but a dynamic process shaped by the interaction between the individual and the environment. Adversity acts as a trigger for activating and developing adaptation mechanisms, and the ability to effectively cope with such situations reflects the level of resilience. This process is influenced by internal factors such as self-esteem, emotional self-regulation, or problem-solving skills, as well as external factors like social support, family climate, or community resources. Therefore, resilience should be understood as a complex interaction between vulnerability and protection, and its assessment involves considering the context in which the adaptive response occurs, not just the exposure to risk.

Adversity is defined as being related to negative life events or circumstances associated with adaptation difficulties (Fletcher, Sarkar, 2013). Other researchers define adversity as any distress linked to difficulty or, taking a broader view, prefer to include both major negative life events and daily challenges (Davis et al., 2009). Existing definitions associate negative circumstances with negative outcomes or risk-related terminology, focusing on statistically significant predictors of maladaptive behavior. Moreover, seemingly positive life events that are not linked to meaningful outcomes may also be relevant to defining resilience.

Further, in their role as guest editors of a special issue of the *“Journal of Personality on Resilience in Common Life”*, Davis Luecken and Lemery-Chalfant (2009) noted that most adversities for the majority of people are not major disasters but rather modest disruptions embedded in daily life. Together with other contributors, they strongly advocate for examining the processes underlying positive adaptation when facing ongoing, demanding daily stressors. Resilience mechanisms may vary depending on the context’s severity – from daily hassles and workplace stress (mild adversity) to intense but occasional stressors like the death of a loved one (severe adversity).

The conceptualization of a positive outcome or adaptation that equates to maintaining mental health and not succumbing to psychological illness after a crisis involves returning to or surpassing one’s previous level of functioning. To demonstrate this, Luthar, Cicchetti, and Becker (2000) argued that the indicators used to represent the concept must correspond to the adversity examined, in both content and methodological rigor.

Another important, yet often overlooked aspect in studying positive adaptation is the sociocultural context in which the individual functions. This view is supported by Mahoney and Bergman (2002), who state that specific sociocultural conditions must be taken into account when examining the phenomenon.

Based on the critical review by Fletcher and Sarkar (2013), an integrative definition can be proposed: psychological resilience is the dynamic capacity for positive adaptation in the face of adversity, resulting from the interaction of individual and contextual factors, and involves the proactive development of psychological resources that protect against stress and enable personal growth even under pressure.

THE IMPORTANCE OF RESILIENCE IN THE MILITARY ENVIRONMENT

The development of psychological resilience is a fundamental component in training future military leaders. Leadership roles in the military inherently involve high-stakes decisions, operational uncertainty, and acute psychological stress. In this context, resilience serves as a core competency that enables leaders to maintain emotional balance, cognitive clarity, and ethical integrity under pressure (Bartone, 2006). Resilient leaders are better prepared to lead by example, demonstrating self-control and adaptability in adverse situations. Their ability to remain functional and supportive contributes directly to unit cohesion and the psychological safety of subordinates. As Meredith et al. (2011) emphasize, leadership-level resilience has a positive ripple effect on collective morale and operational performance, making it not only an individual asset but a strategic necessity.

Furthermore, resilience reduces the likelihood of burnout and cognitive overload – factors that can impair judgment and increase mission failure risk. Preventive programs such as stress inoculation training, as described by Hourani et al. (2011), have proven effective in strengthening coping mechanisms before deployment, contributing to the mental preparedness and psychological durability of leaders.

Beyond performance and endurance, resilience plays a crucial role in maintaining ethical decision-making in morally ambiguous environments. According to Papazoglou et al. (2020), unresolved moral tensions may contribute to post-traumatic stress disorders and moral injury, especially in roles involving life-impacting decisions. Resilient leaders are more likely to act in accordance with military values and uphold professional standards even in the most difficult circumstances.

In conclusion, resilience is not a fixed personality trait but a dynamic capacity that must be cultivated through training, mentorship, and institutional support.

Equipping future military leaders with this ability is essential not only for their psychological health but also for the overall effectiveness and integrity of the military institution.

COMPARATIVE STUDY ON THE RESILIENCE OF MILITARY STUDENTS

This study aimed to comparatively analyze the level of resilience among first- and third-year students at the “*Nicolae Bălcescu*” Land Forces Academy in Sibiu. The comparison allows us to examine whether academic and military training influences the development of resilience in these students. To achieve this, we employed the *College Students’ Resilience Scale* (Wu, Yin, 2022), which includes four dimensions: self-efficacy and adaptability, perception and use of social support, positive cognition, and the ability to adapt to negative emotions. Each dimension consists of a variable number of items, ranging from 4 to 9. Using Google Forms, the questionnaire was distributed online, and the data were later analyzed using the SPSS software.

Research Objectives and Hypotheses

The general objective of this study is to conduct a comparative analysis of resilience levels, evaluated across four essential dimensions: self-efficacy and adaptability, perception and use of social support, positive cognition, and the ability to manage negative emotions. The comparison is made between first- and third-year students at the “*Nicolae Bălcescu*” Land Forces Academy in Sibiu. In line with this research direction, the working hypothesis is that third-year military students demonstrate higher resilience levels across all four dimensions compared to their first-year peers.

Population and Sampling

The research population consisted of 658 students from the “*Nicolae Bălcescu*” Land Forces Academy in Sibiu, enrolled in the first and third years of study. To determine the sample size, the Taro Yamane (1967) sampling formula was applied, with a 5% accepted margin of error. This approach allows the selection of a statistically representative sample of the target population, ensuring an adequate level of accuracy in estimating results.

Resilience Among Future Military Leaders
– Comparative Study Among the Students of the “Nicolae Bălcescu” Land Forces Academy –

Table 1: Number of students by academic year

Academic Year	Total Students	Sample Size
Year 1	365	277
Year 3	293	231
Total	658	508

Subsequently, the proportion of students was determined by year, faculty (across the academy’s three faculties), and military specialization, using stratified sampling. For this paper, we present data related to the Bachelor’s program in *Military Leadership* from the Faculty of Military Sciences, focusing on the two years of study (*Table 2 and 3*). As a result, our sample includes 81 first-year students and 69 third-year students in the Military Leadership program.

Table 2: Distribution of first-year Military Leadership students by specialization

Specialization	Percentage	Number of Students
Infantry	75,75%	60
Reconnaissance	24,25%	21
Total	100%	81

Subsequently, the proportion of students was determined by year, faculty (across the academy’s three faculties), and military specialization, using stratified sampling. For this paper, we present data related to the Bachelor’s program in *Military Leadership* from the Faculty of Military Sciences, focusing on the two years of study (see *Table 3 and Table 4*). As a result, our sample includes 81 first-year students and 69 third-year students in the Military Leadership program.

Table 3: Distribution of third-year Military Leadership students by specialization

Specialization	Percentage	Number of Students
Infantry	60,90%	42
Reconnaissance	31,88%	19
Mountain Troops	7,22%	8
Total	100%	69

Data Analysis

The analysis of responses reveals a generally favorable level of psychological resilience among students, with high average values on the dimensions of self-efficacy and adaptability ($M = 3.68$), perception of social support ($M = 3.49$),

and positive cognition ($M = 3.48$). These results indicate that most students demonstrate important adaptive resources in terms of confidence in their own abilities, effective use of their social support networks, and positive cognitive strategies when facing challenges. However, the dimension with the lowest average ($M = 2.27$) was the ability to adapt to negative emotions, suggesting emotional vulnerabilities in managing negative affective states such as depression or difficulty in regulating anger. This profile highlights the need to pay particular attention to the development of emotional regulation and affective coping skills in order to fully strengthen the psychological resilience of students in the demanding military environment.

First- and third-year students obtained the following averages for the four dimensions of resilience (self-efficacy and adaptability, perception and use of social support, positive cognition, and the ability to adapt to negative emotions) (*figure 1*):

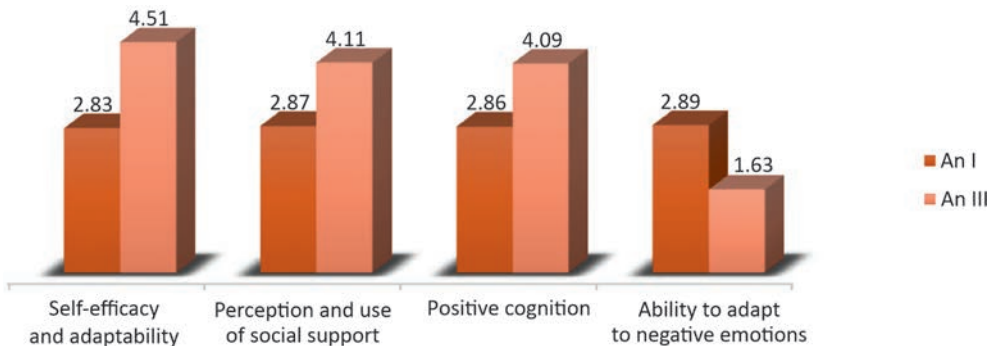


Figure 1: Average scores for each resilience dimension (self-efficacy and adaptability, perception and use of social support, positive cognition, ability to adapt to negative emotions) among first- and third-year students (author's conception)

Comparative results show a significant differentiation between first- and third-year students across all four dimensions of resilience. Third-year students exhibit higher levels of self-efficacy and adaptability ($M = 4.51$ vs. $M = 2.83$), perception and use of social support ($M = 4.11$ vs. $M = 2.87$), and positive cognition ($M = 4.09$ vs. $M = 2.86$). These data suggest a progressive development of adaptive resources over the years of military training, confirming the formative effect of the institutional environment and practical experiences on the consolidation of psychological resilience.

Interestingly, for the ability to adapt to negative emotions, a reversed interpretation trend is observed: the lower average recorded in the third year ($M = 1.63$) compared to the first year ($M = 2.89$) actually indicates an improvement in emotional regulation as students advance in their military training. This positive

evolution suggests a gradual development of emotional coping competencies, likely influenced by adaptation to military rigor, personal maturity, and accumulated experience.

Overall, the results confirm not only an increase in self-efficacy, social support, and positive cognition, but also a significant strengthening of emotional resilience over time. Comparing overall resilience scores between first- and third-year students indicates a favorable evolution throughout military training. The higher general average recorded in the third year ($M = 3.18$), compared to the first year ($M = 2.86$), reflects the gradual consolidation of psychological adaptation capacities, emotional self-regulation, use of social support, and positive cognitive reframing when facing difficulties.

This progress suggests the effectiveness of military training in developing student resilience, through gradual exposure to challenges specific to the military environment, practical experience accumulation, and the formation of complex competencies necessary for adapting to demanding situations.

In a specific context such as the military, developing the ability to efficiently manage stress, pressure, and uncertainty is an essential component of preparing future officers. Understanding the psychological and social mechanisms that support resilience allows for the adoption of educational and organizational measures that contribute to strengthening students' mental and behavioral resistance to the challenges of a military career.

Understanding the motivations behind the actions undertaken by students, whether in the first or third year, can represent an important factor for the military organization. This understanding allows identification of strengths and weaknesses in the leadership training process and supports the development of new programs aimed at increasing resilience levels.

Building resilience among military students through formal education is crucial for preparing a generation of leaders capable of handling operational and psychological challenges specific to the military environment. In a professional context where exposure to stress, uncertainty, and high-pressure decision-making is constant, the early development of adaptation capacities, emotional self-regulation, and flexible thinking becomes a key component of military training.

Formal education not only serves to transmit technical and tactical knowledge but also to build the psychological resources necessary for mental resilience, ethical leadership, and sustainable performance under adversity. By consciously integrating resilience training into the military curriculum, military education institutions can significantly enhance operational preparedness and safeguard the mental health of future officers.

CONCLUSION

The military environment constitutes a distinctive framework for the development of resilience. Exposure to controlled stressful situations, collective responsibilities, and performance pressure fosters the formation of functional coping mechanisms and a high level of frustration tolerance. At the same time, the hierarchical structure and the social support characteristic of military communities contribute to the creation of a sense of belonging and solidarity – factors recognized for their protective role in maintaining mental health. Thus, the military environment can be viewed both as a source of stress and as a context for adaptive psychological development, depending on individual resources and the availability of institutional support.

Although resilience training is recognized as essential for military students, a fundamental question remains as to what extent current educational programs fulfill this objective. The formal military curriculum provides a rigorous framework for physical, theoretical, and tactical training, but the psychological component – especially the development of resilience – is often addressed peripherally or implicitly. Resilience formation is not limited to exposure to difficulties or high standards; rather, it requires deliberate educational interventions focused on developing coping skills, emotional self-regulation, ethical decision-making under pressure, and maintaining motivation under adverse conditions (Bartone, 2006).

Understanding how resilience is formed and manifested at this stage (young cadets) has direct implications for professional success, motivation for a military career, and the emotional stability of future leaders. Continuing the research would allow not only the identification of the cultural and institutional particularities of resilience development but also the design of training and psychological counseling programs tailored to the specific needs of this group. Thus, such research would contribute to strengthening the national scientific database and to formulating effective intervention strategies aimed at supporting adaptation and performance within the military environment.

In this regard, educational programs should be evaluated and adapted to include explicit pedagogical strategies for cultivating resilience: resilience training, realistic simulations with psychological feedback, mentoring, emotional intelligence development, and the integration of applied psycho pedagogical modules. Without a conscious and systemic approach, resilience formation risks remaining a by-product rather than a deliberately formed competence through education.

Therefore, a curricular and methodological reconsideration may be necessary so that resilience becomes an explicit and sustained educational objective in military education – not merely a secondary outcome of academic rigor and institutional discipline.

BIBLIOGRAPHY:

1. Bartone, P.T. (2006). *Resilience under military operational stress: Can leaders influence hardiness?*, in *Military Psychology*, 18 (Suppl), S131–S148, <https://doi.org/10.1207/s15327876mp1803s.10>, retrieved on 12 August 2025.
2. Davis, M.C., Luecken, L.J., Lemery-Chalfant, K. (2009). *Resilience in common life: Introduction to the special issue*, in *International Journal of Environmental Research and Public Health*, 6(7), 1961-1970.
3. Demerouti, E., Bakker, A.B., Nachreiner, F., Schaufeli, W.B. (2001). *The job demands-resources model of burnout*, in *Journal of Applied Psychology*, 86(3), 499-512, <https://doi.org/10.1037/0021-9010.86.3.499>, retrieved on 12 August 2025.
4. Fletcher, D., Sarkar, M. (2013). *Psychological resilience: A review and critique of definitions, concepts, and theory*, *European Psychologist*, 18(1), 12-23, <https://doi.org/10.1027/1016-9040/a000124>, retrieved on 22 August 2025.
5. Hourani, L., Kizakevich, P., Hubal, R., Spira, J., Strange, L., Holiday, D.B., Bryant, S.&McLean, A.N. (2011). *Predeployment stress inoculation training for primary prevention of combat-related stress disorders*, in *Journal of Cyber Therapy and Rehabilitation*, 4(1), pp. 101-119.
6. Luthar, S.S., Cicchetti, D., Becker, B. (2000). *The construct of resilience: A critical evaluation and guidelines for future work*, *Child Development*, 71(3), ppp. 543-562, <https://doi.org/10.1111/1467-8624.00164>, retrieved on 13 August 2025.
7. Mahoney, J.L., Bergman, L.R. (2002). *Conceptual and methodological considerations in a developmental approach to the study of positive adaptation*, in *Journal of Applied Developmental Psychology*, 23(2), pp. 195-217, [https://doi.org/10.1016/S0193-3973\(02\)00105-0](https://doi.org/10.1016/S0193-3973(02)00105-0), retrieved on 22 August 2025.
8. Meredith, L.S., Sherbourne, C.D., Gailliot, S.J., Hansell, L., Ritschard, H.V., Parker, A.M.&Wrenn, G. (2011). *Promoting psychological resilience in the U.S. military*. *RAND Health Quarterly*, 1(2), 2, <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4945176/>, retrieved on 12 August 2025.
9. Papazoglou, K., Blumberg, D.M., Chiongbian, V., Tuttle, B. , Kamkar, K., Chopko, B., Milliard, B., Aukhojee, P.&Koskelainen, M. (2020). *The role of moral injury in PTSD among law enforcement officers: A brief report*, in *Frontiers in Psychology*, 11, 310, <https://doi.org/10.3389/fpsyg.2020.00310>, retrieved on 22 August 2025.
10. Wu, Y. (2022). *Development of College Students' Resilience Scale*. In *BioMed Research International*, 1-7. 10.1155/2022/8418279.
11. Zolli, A., Healy, A.M. (2012). *Resilience: Why things bounce back*. New York, NY: Simon&Schuster.

PUBLIC GOODS AND PUBLIC POLICIES IN THE FIELD OF SECURITY: THE INTERSECTION BETWEEN ECONOMY AND DEFENCE STRATEGY IN THE CONTEXT OF CONTEMPORARY TRANSFORMATIONS

Major Daniel-Dorin CUCURĂ

*The 405th Logistic Support Battalion "Năsăud",
Doctoral Student at The Doctoral School of Administration and Public Policies,
Faculty of Political, Administrative and Communication Sciences,
"Babeş-Bolyai" University, Cluj-Napoca
DOI: 10.55535/RMT.2025.3.35*

This article examines security as a national and global public good, positioning it at the intersection between the economy and defence strategy. The central objective is to analyse how economic resources and available infrastructures shape military capabilities and, conversely, how defence strategies sustain the stability required for economic development. Methodologically, the research combines a theoretical analysis of the specialised literature on public goods and public policies with an applied examination of the contemporary context, including the COVID-19 pandemic and the conflict in Ukraine. The findings show that security goes beyond its traditional military dimension, encompassing health, energy, cyber and societal aspects, which assigns public administration the role of orchestrator of resources and international cooperation. The case studies confirm that investments in defence, resilience and emerging technologies contribute simultaneously to security and economic development.

The contribution of this paper lies in articulating an integrated perspective on security as a public good, supported by coherent public policies and international partnerships. The conclusions and recommendations target decision-makers and practitioners in public administration and security, suggesting directions for governance adapted to contemporary transformations.

Keywords: national security; public goods; public policy; military strategy; economy and defence;

INTRODUCTION

The accelerated transformations of the international security environment over the past decades have profoundly redefined how states and international organisations understand and manage security issues. Emerging technologies – from artificial intelligence to autonomous systems and biotechnologies – together with geopolitical changes and recent global crises have extended the concept of security beyond the strictly military dimension. Security must therefore be regarded as a fundamental public good that encompasses health, energy, cyber and social dimensions. Public administration is at the core of this process, tasked with ensuring policy coherence, allocating resources and stimulating inter-institutional and international cooperation.

Starting from the premise that security is inseparably linked to the economy, this study aims to highlight the interdependence between economic resources and available infrastructures on the one hand and military strategies on the other. Financial resources, critical infrastructures, human capital and innovation capacity define the possibilities and limitations of building defence capabilities. Conversely, internal and external security and stability generate the conditions necessary for investment, trade and sustainable development. The COVID-19 pandemic and the conflict in Ukraine have clearly shown that economic and social vulnerabilities rapidly turn into security risks and that a lack of effective coordination can amplify their impact.

The paper proposes a dual approach: on the one hand, from a theoretical perspective, security is addressed through the lens of public good and public policy theories, with an emphasis on its characteristics of non-excludability and non-rivalry; on the other hand, the applied part focuses on how the economy directly influences contemporary military strategies, illustrated by relevant case studies on Romania, NATO, the EU and global implications. The article ends with a set of conclusions and recommendations designed to provide useful benchmarks for decision-makers in public administration structures to adapt governance to the challenges of contemporary transformations.

In light of these considerations, a solid theoretical foundation is needed to explain how security can be conceptualised as a public good and to outline the public policy instruments through which it is provided.

The pace of change in the security environment has accelerated significantly in the last decade, driven by the convergence of technological progress (artificial intelligence, automation, biotechnologies), geopolitical shifts (redistribution of power, the return of great-power competition) and systemic crises (COVID-19, the conflict in Ukraine). The “*new revolution in military affairs*” is no longer merely technological but also organisational, doctrinal and social, requiring a reconfiguration of the role of public administration in managing security as a public good.

Against this background, the emphasis falls on governance, on the ability of public institutions to coordinate resources, on cooperation within alliances and on societal resilience. Equally important is the integration of cyber, energy and health dimensions into the broader concept of security, moving beyond the strictly military logic. National and international security is a public good with properties of non-excludability and non-rivalry (Samuelson, 1954), which has two main consequences for public administration:

- (I) *the state becomes the provider of last resort of security;*
- (II) *inter-institutional and international coordination is indispensable for managing externalities and cross-border risks.*

Public policies in the field of security must balance allocative efficiency with democratic legitimacy and the protection of rights. In this context, the emphasis is on governance, on the capacity of public institutions to coordinate resources, on cooperation in alliances and on societal resilience. It is equally essential to integrate cyber, energy and health dimensions into the broad concept of security, moving beyond the strictly military logic.

The paper investigates the intersection between the economy and defence strategy: how economic resources and available infrastructures condition strategic options, and how strategic choices shape the economic structure and development trajectory. Methodologically, we adopt a dual approach consisting of a theoretical framework (public goods, public policies, political economy of security) and an applied analysis with case studies (Romania, NATO, EU, lessons from the pandemic and the conflict in Ukraine), integrating comparative and institutional perspectives.

PUBLIC GOODS AND PUBLIC POLICIES IN THE FIELD OF SECURITY

The theoretical analysis of security as a public good starts from the fundamental concepts formulated in the specialised literature. Public goods are defined by their characteristics of non-excludability and non-rivalry, as emphasised by Samuelson (1954) and later developed by Musgrave (1959). This category includes goods which, once provided, can not exclude beneficiaries, and whose use by one individual does

not reduce availability for others. National security corresponds to this pattern, since the protection provided by the state is felt by all citizens regardless of their individual contribution.

Subsequent developments have nuanced this perspective by introducing notions such as club goods (Buchanan, 1965), which are excludable but non-rival up to a certain congestion threshold, and common-pool goods (Ostrom, 1990), characterised by open access but at risk of over use. More recently, the concept of global public goods (Kaul et al., 2003) has offered a useful framework for understanding security at the transnational level, where threats such as international terrorism, climate change or financial instability can not be managed exclusively by a single state.

A central element of the theoretical debate is the “*free rider*” problem, analysed by Olson (1965). This explains the tendency of actors to underfund public goods while benefiting from the contributions of others. In the security field, the phenomenon is visible in alliances, where fair burden-sharing represents a constant challenge. Institutional mechanisms and international norms play a role in limiting opportunistic behaviour and ensuring the cooperation needed for the provision of collective security.

With regard to public policies, they follow a specific cycle: problem identification, formulation of solutions, implementation of measures and evaluation of results. The classical model of the policy cycle (Dunn, 2017) has been adapted in the security field through the integration of risk management and resilience. Thus, public administration structures must be able to rapidly identify new types of threats, formulate effective responses, mobilise resources and evaluate the impact of implemented policies. All these stages require a high degree of coordination between national institutions and international partners.

The ethics of security constitutes another essential dimension of the theoretical framework. The provision of security can not be separated from respect for the rule of law and the fundamental rights of citizens. Civilian control over the armed forces, decision-making transparency and institutional accountability are indispensable conditions for the democratic legitimacy of security policies. Security is the refore not only a technical objective but also a deeply political and normative one.

Overall, the theoretical framework presented demonstrates that security needs to be viewed as a complex public good, located at the intersection of economic needs, strategic imperatives and ethical constraints. These theoretical foundations form the basis for the applied analysis in the next chapter, where the interaction between the economy and defence strategy is detailed through case studies and practical examples.

The Theory of Public Goods: Definitions and Extensions

The concept of the public good has become a fundamental benchmark of modern economic theory. In its classical form, developed by Paul Samuelson (1954) and further elaborated by Richard Musgrave (1959), public goods are those goods or services simultaneously characterised by **non-excludability** and **non-rivalry**. Non-excludability means that, once the good is provided, it is not possible – or is very costly – to exclude certain individuals from consuming it. Non-rivalry implies that the use of the good by one individual does not diminish its availability for other members of the community. Classic examples include street lighting, national defence or floodprotection.

Later literature has refined this category. Buchanan (1965) introduced the concept of **club goods**, that is, goods which are in principle non-rival but to which access can be restricted to members of a group paying a fee (such as toll motorways or cable networks). He showed that, through voluntary association, individuals can share the costs of providing a non-rival good and limit access to avoid congestion.

Elinor Ostrom (1990), on the other hand, emphasised **common-pool resources** – resources characterised by rivalry but difficult to exclude, such as forests, fishing grounds or underground water. She demonstrated that, in the absence of collective management, these resources can be over used, a phenomenon known as the “*tragedy of the commons*”.

Finally, Kaul and colleagues (2003) extended the perspective by introducing the notion of global public goods to designate those goods whose benefits and costs transcend state borders. Relevant examples include climate stability, international financial security or the fight against global terrorism. This extension underlines that the provision of global public goods requires international cooperation and robust multilateral institutions.

Within this theoretical framework, **security** emerges as a complex and particular example. At the national level, defence and public order can be considered pure public goods, since the protection offered by the state extends to all citizens without discrimination and without additional marginal costs per beneficiary. However, as threats become transnational – international terrorism, cyber-attacks, the proliferation of weapons of mass destruction – security takes on the features of a **global public good**, whose effective provision depends on cooperation between states, military alliances and international institutions.

Thus, the theory of public goods provides not only a conceptual framework for understanding security but also an argument for public policies aimed at sharing responsibilities and resources between national and international actors.

This approach lays the groundwork for the in-depth analysis of the relationship between economy and defence strategy in the following chapters.

The Free Rider Problem and Collective Governance

One of the best-known obstacles to the efficient provision of public goods is the **“free rider” problem** theorised by Mancur Olson (1965). This describes the tendency of actors – whether individuals, organisations or states – to benefit from a public good without contributing proportionally to its costs. Because public goods are characterised by non-excludability, each participant has an incentive to reduce their own contribution, hoping that others will cover the costs while they enjoy the benefits free of charge. The result, in the absence of corrective mechanisms, is underfunding and insufficient provision of the good in question.

In the field of international security, the free rider problem is particularly evident in **military alliances**. Mechanisms such as NATO involve burden sharing among members for financing common capabilities, participating in operations and maintaining interoperability. In practice, however, some states tend to contribute less than others, relying on the protection offered by stronger allies. This asymmetry creates political tensions and can undermine the cohesion of the alliance in the long term, especially when costs increase or threats diversify.

Collective governance thus emerges as a necessary response to limit opportunistic behaviour. It relies on **rules, norms and institutions** that establish mutual expectations, define contribution criteria and provide monitoring and sanctioning mechanisms. In NATO, for example, the agreed target of allocating 2% of GDP to defence functions as a shared norm, intended to encourage convergence of efforts and reduce the free-riding phenomenon. Transparent reporting of expenditure, periodic capability assessments and integrated planning also contribute to holding member states accountable.

Beyond military alliances, collective governance also encompasses **multilateral institutions and international agreements** managing global public goods, such as non-proliferation regimes or cooperation in the cyber domain. Establishing common standards, verification procedures and mutual support mechanisms helps to create an atmosphere of trust and reduce opportunistic behaviours.

Thus, the free rider problem and collective governance solutions are inseparable in analysing security as a public good. They explain why the mere existence of a common interest is not sufficient for cooperation and why institutions, rules and norms are essential for the effective provision of security at national, regional and global levels. This perspective sets the stage for the discussion of concrete

instruments through which public administrations can stimulate equitable participation and ensure the sustainability of alliances and partnerships in the field of security.

Public Policies: The Policy Cycle and Instruments

The analysis of security as a public good can not be complete without a clear understanding of **the process of designing and implementing public policies**. The classical model of the policy cycle, described by Dunn (2017), offers a useful conceptual framework for capturing decision-making dynamics. This model identifies four main stages – *problem definition, policy formulation, implementation and evaluation* – which, although presented sequentially, in practice overlap, recur and are continually adjusted. In the field of security, this flexibility is essential because the strategic environment is marked by uncertainty, rapid change and the emergence of new threats.

The first stage, **problem definition**, involves recognising and precisely delineating the risks and vulnerabilities that affect national or international security. At this stage, public administration must mobilise multidisciplinary expertise and consult relevant actors in order to understand the root causes of threats. Without proper diagnosis, policies risk being reactive and ineffective.

The second stage, **policy formulation**, entails the development of response options and the selection of appropriate instruments. Here institutional creativity comes into play and the ability to combine different types of tools: regulation, taxation, subsidies, contracting, public-private partnerships or direct investment in capabilities. In the security domain, instruments can include the elaboration of doctrines and strategies, capability planning, procurement and modernization programmes, as well as measures of international cooperation, strategic education or public communication to strengthen societal support.

The third stage, **implementation**, turns political decisions into concrete actions. This requires interinstitutional coordination, efficient resource management and continuous progress monitoring. In security, implementation is reflected in the conduct of military exercises, the commissioning of critical infrastructure, the completion of procurement processes or the operation of training and strategic education programmes.

Finally, **policy evaluation** plays the role of measuring the efficiency, effectiveness and impact of actions undertaken. It provides feedback for the adjustment of future decisions and contributes to institutional learning. In the security field, evaluation may take the form of capability audits, after-action reviews or periodic reports to national and international bodies.

Throughout this cycle, **the choice of instruments** is very important. There is no universal set of tools suitable for all situations; public administration must adapt the policy mix according to the nature of the threat, the resources available and the international framework. In the case of security, this may mean combining investments in emerging technologies with strengthening public-private partnerships, reinforcing the regulatory framework and developing a strategic culture among personnel and the wider population.

Thus, the policy cycle model and the diversity of available instruments provide an essential framework for the governance of security as a public good. They show that the success of policies depends not only on the formulation of ambitious objectives but also on rigorous implementation, continuous adaptation to changes in the strategic environment and ongoing evaluation of results.

Public Administration and Risk Management

In the context of accelerated transformations and complex threats, public administration faces a reality characterized by uncertainty, volatility and multiple interdependencies. Traditionally, public institutions were mainly oriented toward linear planning and responding to predictable events. At present, however, this approach is no longer sufficient. Risk and **resilience management** are becoming central tools for prioritizing interventions and allocating resources efficiently in the face of diverse and often unpredictable threats.

Risk management involves identifying, assessing and addressing potential hazards before they materialize. In the security field, this process covers not only traditional military risks but also those associated with public health, cybersecurity and energy. Integrated management of these risks allows proactive planning, reduction of vulnerabilities and the creation of rapid response mechanisms. At the same time, resilience complements risk management: it refers to the ability of public and private systems to absorb shocks, adapt and return to normal functioning after a disruption.

In this context, **“all-hazards”** models are attracting increasing attention. These propose an integrated approach to all types of risks, regardless of their source, avoiding fragmentation by sector or agency. Through this model, public administration develops standardized plans and procedures applicable to a wide range of emergency situations, whether pandemics, cyberattacks or natural disasters. A major advantage of the **“all-hazards”** approach is efficiency: instead of preparing separate plans for each type of risk, institutions build versatile capabilities adaptable to multiple scenarios.

In parallel, the *“whole-of-government/whole-of-society”* model reflects the need for interinstitutional coordination and the active involvement of all societal actors. *“Whole-of-government”* entails close collaboration between different ministries and governmental agencies, overcoming traditional institutional silos. *“Whole-of-society”* extends this logic by involving the private sector, non-governmental organizations, academia and citizens in the development and implementation of security policies. This model recognizes that, in the face of complex threats –from cyber attacks to energy and health crises – no single actor possesses all the necessary resources and expertise.

Applying these models in public administration has direct consequences for **national security policies**. For example, integrating health, cyber and energy security into a coherent strategy requires coordination mechanisms, information sharing and joint exercises between institutions. At the same time, risk management must be accompanied by strategic communication and public education so that citizens understand the measures taken and contribute to collective resilience.

Therefore, public administration becomes not only a provider of services, but also an orchestrator of a **national security ecosystem** in which the public sector, private sector and civil society collaborate to prevent and manage risks. Risk and resilience management, applied within the *“all-hazards”* and *“whole-of-government/whole-of-society”* frameworks, represents an indispensable pillar of modern security policies.

Ethics of Security and Democratic Legitimacy

In a democratic society, **the provision of security** can not be separated from respect for the rule of law and the protection of fundamental civil rights. Although the need for protection against internal and external threats may lead governments to adopt firm measures, these measures must be designed and implemented in ways compatible with democratic principles. Transparency, accountability and civilian control over the armed forces constitute the pillars of legitimacy. Their absence can lead to abuses of power, loss of public trust and even the undermining of long-term security.

Transparency in the field of security implies clear communication of objectives, budgets and policy results in a manner that does not compromise sensitive aspects but that gives citizens and their representatives the ability to understand and evaluate the actions taken. **Accountability** requires mechanisms through which decision-makers and institutions are held responsible for errors or abuses, including through audits, public reports or independent investigations. **Civilian control** over the armed forces represents a fundamental guarantee of democracy: the military

and security structures must serve the interests of society under the authority of elected leaders, rather than be coming an autonomous actor in the political process.

However, security policies often involve sensitive information, discreet operations and plans that can not be made public without affecting their effectiveness. **The challenge of democratic governance** lies precisely in finding a balance between the **necessity of secrecy** – indispensable for protecting operations and sources – and the **democratic requirements of oversight and control**. The experience of mature democracies shows that this balance can be achieved through independent oversight institutions, specialised parliamentary committees, regular public reporting and a culture of integrity within security institutions.

This ethical approach is also relevant for **extending the concept of security** beyond the military domain. While national defence, public order and civil protection can be considered pure public goods provided by the state, areas such as cyber, energy, health or food security have the features of mixed goods, requiring the involvement of the private sector and civil society. At the global level, phenomena such as climate change, international terrorism or financial instability represent global public goods whose efficient provision depends on the cooperation of international institutions such as NATO, the European Union or the United Nations.

Thus, we can outline a **conceptual framework** that reflects this diversity: national security (pure public good) encompasses defence, public order and civil protection; extended security (mixed goods) includes areas such as cyber, energy, health and food; global security (global public good) refers to climate, international terrorism and financial stability. The instruments through which these levels are managed range from public policies and budgetary resources to mechanisms of cooperation and institutional partnerships.

Finally, the **theoretical foundations** presented in this first chapter provide an interpretative framework necessary for analysing the practical dimensions of security. They show that moving from conceptualisation to reality involves observing how economic resources and available infrastructures shape defence strategies, and how recent transformations – such as the COVID-19 pandemic or the conflict in Ukraine – have shaped security policies. The next chapter illustrates these relationships through relevant examples and case studies, preparing the ground for public policy recommendations.

Architecture of Public Security Goods

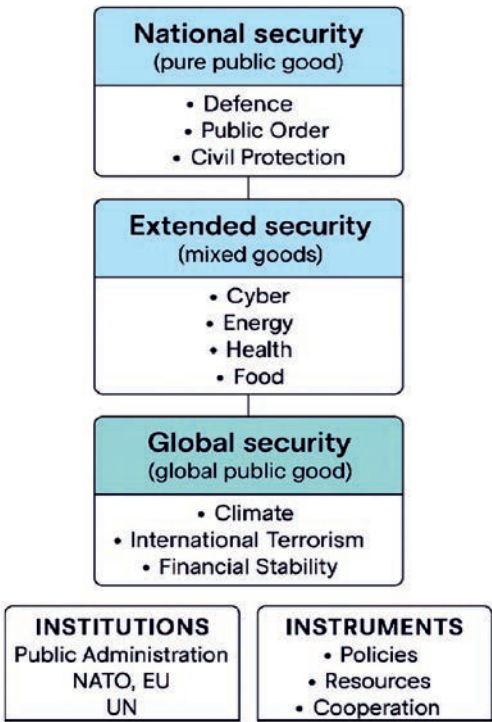


Figure 1: Architecture of Public Security Goods

As shown in *Table 1*, the types of public goods relevant to security can be described in a continuous manner so as to highlight the transition from the national to the global level and the nature of the instruments used.

Table 1: Types of Public Goods Relevant for Security

Type	Characteristics	Examples in Security	Policy Implications
Pure public good	Non-excludable, non-rival	Territorial defence	Collective budgetary funding
Global public good	Transnational	Climate stability, counterterrorism	International cooperation
Club good	Excludable, non-rival until congestion	Common capabilities in an alliance	Contributions and access rules
Common-pool good	Non-excludable, rival	Electromagnetic space, spectrum	Usage rules, monitoring

At the **national level**, security is structured around pure public goods provided by the state: defence, public order and civil protection. These areas are non-excludable and non-rival: the protection offered by the army, police or emergency services extends to the entire population regardless of individual contribution. Public administration is responsible for planning, financing and coordinating these functions, thereby ensuring a minimum guaranteed level of security for all citizens.

As the concept of security **expands**, domains with the characteristics of mixed goods emerge, where effective provision requires collaboration between the public and private sectors. Cybersecurity, energy security, public health and food security are relevant examples. In these cases, non-excludability is no longer absolute, and rivalry may arise under conditions of crisis or overload. Therefore, governance is based on public-private partnerships, regulation, common standards and coordinated investments to maintain access to and the functionality of these essential goods.

At the **global level**, security takes on the characteristics of a global public good. Phenomena such as climate change, international terrorism or financial instability can not be effectively managed by a single state. They simultaneously affect multiple regions and generations and require sustained multilateral cooperation. International institutions – NATO, the European Union and the United Nations – become platforms through which states coordinate their policies, mobilise resources and create common norms for the provision of these global goods. The instruments used range from treaties and international agreements to joint programmes, pooled funding and stabilisation missions.

This narrative presentation allows a gradual understanding of the types of public goods relevant to security, highlighting the continuity between the national, extended and global levels and clarifying the role of public administration and international institutions in their provision.

The Relationship between Public Administration and National/International Security

Public administration represents the institutional infrastructure through which the state exercises its essential functions, including the provision of security as a public good. At the national level, the administration plays the role of designing policies, mobilising resources and coordinating the institutions responsible for defence, public order and civil protection. This role is not purely technical but involves making strategic decisions that affect the balance between freedom and security, transparency and secrecy, and social costs and benefits (Rothstein, 2011).

In a consolidated democracy, public administration acts as an **intermediary between political decision-makers and citizens**, ensuring that security policies reflect both public will and the international commitments undertaken by the state. It is responsible for formulating national defence strategies, managing risks and implementing international standards. For example, in Romania, the Ministry of National Defence and the Ministry of Internal Affairs act on the basis of government plans approved by Parliament and coordinated with NATO and EU strategies (Government of Romania, 2022).

At the international level, **security can no longer be provided unilaterally**. Transnational threats – terrorism, organised crime, cyberattacks, climate change – require cooperation between states and institutions. National administrations thus become key actors in **global governance networks**, contributing data, expertise and resources to collective security mechanisms (Keohane, Nye, 2001). Participation in organisations such as NATO, the European Union or the United Nations involves not only assuming formal obligations but also adapting internal administrative structures to cooperate effectively with external partners.

This bidirectional relationship between public administration and national/international security entails a series of challenges. First, **resource allocation**: administrations must balance defence expenditure with domestic social and economic needs. Second, **inter-institutional coordination**: modern security covers multiple dimensions – military, economic, health, cyber – that require collaboration between ministries, agencies and the private sector. Third, **democratic legitimacy**: the involvement of the administration in international security mechanisms must be transparent and comply with the rule of law and parliamentary oversight (Born et al., 2003).

Therefore, public administration is not merely an executor of political decisions in security matters but a **strategic actor** that shapes defence policy, coordinates the implementation of international obligations and mediates the relationship between state and citizen. In the context of contemporary transformations, the success of security policies depends on the capacity of administrations to integrate national and international perspectives, anticipate risks and build systemic resilience through coherent policies and durable partnerships.

ECONOMY AND MILITARY STRATEGY IN THE CONTEMPORARY CONTEXT

Where as the first chapter provided the theoretical framework of security as a public good and the instruments through which it can be delivered, this chapter focuses on the **practical dimensions** of the interaction between the economy and military strategy. In the 21st century, economic resources are no longer merely the basis for financing military capabilities but have become a strategic element in their own right, directly influencing national resilience and the cohesion of international alliances.

This section analyses several complementary directions: **economic resources as the foundation of military power**; budgetary policies and NATO's **2% of GDP** defence spending benchmark; and the transformative effects of recent crises. **The COVID-19 pandemic** highlighted systemic vulnerabilities and redefined population health as a strategic element, while the **conflict in Ukraine** brought to the forefront issues of energy security, logistics and doctrinal adaptation. It will also address the **interdependence between the economy and military strategy**, investments in technology, the defence industry and digitalisation, as well as the **role of the European Union and NATO** in managing security-related public goods.

Through this approach, the chapter offers an integrated picture of how current economic realities and geopolitical challenges shape defence strategies and security governance in Romania, in the Euro-Atlantic space and globally.

Economic Resources as the Foundation of Military Power

A state's ability to build, maintain and modernise its armed forces fundamentally depends on the **economic resources** it can mobilise. Since the classic works of international relations, military power has been considered inseparable from economic power, which provides the material basis for financing equipment, training personnel, technological development and the logistical support of operations (Kennedy, 1987). A state with a solid economy can allocate more consistent resources to defence without compromising social welfare, thereby increasing both its deterrence capacity and its resilience to crises.

Traditionally, the **defence budget** reflects a state's strategic priorities and the extent to which it can transform economic potential into military power. NATO states agreed at the 2014 Wales Summit to allocate at least **2% of GDP** to defence by 2024, precisely to ensure the sustainability of collective capabilities (NATO, 2023). This target is not merely an accounting indicator but also a political signal of the willingness to contribute to common security and to avoid the

“free rider” phenomenon described by Olson (1965). Romania, for example, has managed to reach and maintain this level of funding since 2017, which has allowed the accelerated modernisation of its armed forces and more active participation in international missions (Government of Romania, 2022).

Economic resources, however, are not limited to annual budgets. **The structure of the economy** and its **critical infrastructures** directly influence mobilisation capacity in times of crisis. A diversified industrial base, robust supply chains and a skilled workforce enable the rapid production of necessary equipment and long-term logistical support. Lessons from the two World Wars show that states capable of converting civilian industries into war industries held a decisive advantage (Tooze, 2006). Today, this logic underpins the emphasis on **dual-use capabilities** and on public-private partnerships for the development of technologies with simultaneous civilian and military applications (Edwards, 2018).

At the same time, **macroeconomic stability** is a prerequisite for sustainable defence financing. Excessive budget deficits or financial crises can drastically reduce available resources and limit investments in strategic capabilities. The COVID-19 pandemic highlighted this vulnerability: massive spending on public health and economic support competed with defence allocations, while supply-chain disruptions affected military procurement programmes (SIPRI, 2021). These developments confirm that economic resilience is an integral part of national resilience.

Economic resources also form the basis for **investment in research and development**. In the age of emerging technologies – artificial intelligence, autonomous drones, biotechnology, cyber security – military competitiveness depends on states’ ability to finance innovation and integrate results into doctrine and equipment (Gilli, Gilli, 2019). Countries with dynamic technological ecosystems and institutions that facilitate collaboration between universities, industry and the armed forces are better positioned to maintain their strategic advantage.

Finally, economic resources have a **geopolitical** dimension. States with large economies can use aid, credits and investments to build alliances, support partners and project stability in key regions. The financial and logistical support provided to Ukraine by NATO and EU states after 2022 illustrates how collective economic power can be transformed into strategic effect, strengthening the defence of a third state and deterring aggression (European Council, 2023).

Therefore, economic resources are not just a contextual factor but a **structural foundation of military power**. Public administrations must manage this relationship in an integrated manner, balancing domestic social needs with security commitments,

and short-term spending with long-term capability development. The ability to mobilise economic resources efficiently ultimately makes the difference between a declarative defence strategy and a credible one.

Budgetary Policies and National Defence (the Example of 2% of GDP for NATO)

Budgetary policies in the field of defence represent the central instrument through which states transform strategic objectives into concrete capabilities. By allocating financial resources, governments determine not only the level of military preparedness but also the direction of force development and the degree of interoperability with allies. Unlike other public policies, defence budgets have a dual meaning: they are both indicators of internal priorities and external signals of the credibility of security commitments (Smith, 2019).

Within **NATO**, the budgetary dimension has become a criterion of solidarity and equitable burden sharing. At the 2014 Wales Summit, member states pledged to allocate at least **2% of GDP** to defence by 2024, of which at least 20% was to be devoted to major equipment and research & development (NATO, 2023). This commitment has been reiterated at subsequent summits, reflecting consensus that the effective deterrence of contemporary threats requires constant and predictable investment.

For many European states, reaching this threshold has represented a significant change in public policy. Romania, for example, adopted in 2015 a national political agreement committing to increase the defence budget to 2% of GDP starting in 2017 and to maintain this level in the long term (Government of Romania, 2022). This decision enabled the launch of programmes to modernise aviation, air defence and communications, while simultaneously strengthening Romania's credibility within the Alliance.

However, defence budget policy cannot be viewed in isolation. It must be correlated with **fiscal sustainability** and the needs of other public sectors. Massive military expenditures, unaccompanied by economic growth or structural reforms, can generate social tensions and unsustainable budget deficits (Băhnăreanu, 2009). For this reason, governments seek a **balance** between investments in defence and those in civil infrastructure, health or education, thus ensuring political legitimacy and citizen support for security policy.

In addition, budgetary allocation does not automatically guarantee efficient use of funds. **Transparency and accountability** in the execution of the defence budget are essential to avoid waste, corruption and delays in procurement programmes.

In this sense, public audit, regular reports to Parliament and civil society involvement can contribute to improving the performance of defence spending and maintaining public trust (Born et al., 2003).

In the context of recent crises such as the COVID-19 pandemic and the conflict in Ukraine, defence budget policies have acquired an additional dimension: that of **multidimensional resilience**. States have begun integrating into defence planning investments in strategic stockpiles, critical infrastructure and dual-use capabilities, as well as increasing budgets for research in emerging domains from cyber security to biotechnology (SIPRI, 2021). Thus, the 2% of GDP threshold becomes not only a financial target but also a benchmark for the structural transformation of defence policies and for strengthening collective security.

At the NATO Summit in The Hague in June 2025, the Alliance's members adopted a historic decision to increase defence spending: NATO states committed to raise spending—including related security elements – to **5% of GDP by 2035**. Of this amount, **3.5% of GDP** will be dedicated to core military expenditures (equipment, personnel, operations, maintenance) and **1.5%** to “*defence-related*” activities – critical infrastructure, digital infrastructure, resilience (reserves, logistics, innovation, etc.). The decision was approved through a joint investment plan (“*The Hague Investment Plan*”) and provides for intermediate assessments, especially in 2029, to monitor progress and adjust trajectories according to the strategic environment.

The implications of this decision are multiple and unfold at the economic, political and strategic levels. Economically, raising spending to 5% of GDP will put pressure on national budgets, especially for states with deficits, high debt or substantial economies with low productivity; however, simulations show that, if implemented gradually, it can generate positive effects through investment in infrastructure, stimulation of the defence industrial sector, job creation and technological innovation (Janes, 2025). Politically, the decision is a strong signal of unity and determination in the face of the Russian threat but carries a risk of domestic opposition in fiscally vulnerable states or those with strong social priorities. NATO's strategy will need to clarify what is concretely included in the “*defence-related*” component to avoid the use of these expenditures as a form of creative accounting, since effectiveness is not determined only by percentages but by how resources are directed to relevant, interoperable capabilities adapted to current threats.

Romania, which in 2024 allocated approximately **2.2% of GDP** to defence, plans to increase this percentage towards **5%** in the context of NATO's 2025 commitment. According to an **Erste Group** report from 2025, scenarios exist in which Romania

could reach 5% of GDP by 2028 through gradual growth depending on economic performance, revenue increases and the willingness to reallocate budgetary spending (Erste Group, 2025; Romania Insider, 2025).

The fiscal impact of such an increase is significant. Romania is already facing a large government deficit, estimated at over **8.6% of GDP** in 2024. Raising defence spending to 5% of GDP would require an additional budgetary effort, probably in the form of higher fiscal revenues, reductions in other areas of expenditure or the use of EU/externally provided exceptional funds. Economists and financial institutions warn that without fiscal consolidation Romania risks increased public debt and additional pressure on fiscal credibility.

In conclusion, budgetary policies are more than simple accounting allocations; they reflect a state's political will, administrative capacity and strategic vision. Achieving and maintaining an adequate level of defence financing is a necessary but not sufficient condition for an effective security policy. It must be accompanied by rigorous planning, transparency and international cooperation to transform financial resources into real and credible capabilities.

The Impact of the COVID-19 Pandemic on Security

The COVID-19 pandemic represented the most severe test of the resilience of national security systems since the end of the Cold War. Although at first glance a health crisis seems separate from the military domain, the experience of recent years has shown that population health, the functioning of logistics chains and the response capacity of public institutions are **strategic** elements with a direct impact on national and international security (WHO, 2021). COVID-19 demonstrated that economic and social vulnerabilities can be exploited by state or non-state actors and that security must be redefined to include non-military dimensions.

First, the pandemic triggered unprecedented **resource crises**. Public budgets came under enormous pressure due to spending on health, economic support and social protection measures. In many states, defence allocations stagnated or were postponed, affecting procurement programmes and military exercises (SIPRI, 2021). At the same time, travel restrictions and transport blockages disrupted supply chains for the defence industry, delaying the delivery of equipment and limiting the maintenance of existing capabilities (OECD, 2020).

Second, the pandemic highlighted **population health as a strategic element**. The preparedness of the medical system, testing and vaccination capacity, stockpiles of medical materials and inter-institutional cooperation became indicators of national resilience. Armed forces were called upon to support vaccination logistics, transport medical equipment and maintain public order under restrictive conditions,

confirming the interdependence between civil and military security (MAPN, 2021). In theoretical terms, this reflects an extension of the concept of the public good: protecting collective health becomes a precondition for the functioning of security institutions and for national defence.

Third, the pandemic accelerated the **digitalisation and doctrinal transformation** of security institutions. Telework, online communication and data management became essential for the continuity of critical functions. At the same time, cyber-threats increased, exploiting vulnerabilities generated by massive use of digital platforms. This led governments to invest more in cyber security and resilient digital infrastructures, adding a new dimension to defence budgets (ENISA, 2021).

At the international level, the pandemic underscored the need for **multilateral cooperation**. The unequal distribution of vaccines, competition for medical equipment and the use of trade restrictions generated geopolitical tensions, while revisionist actors attempted to exploit these weaknesses to undermine the cohesion of Western alliances (EUISS, 2021). At the same time, NATO and the EU developed mechanisms for coordination and mutual support, demonstrating that international institutions can function as providers of global public goods in the field of health and security.

In conclusion, the impact of the COVID-19 pandemic on security has been **multidimensional**. It has shown that traditional military power is insufficient without functioning critical infrastructures, a healthy population and a resilient economy. The main lesson for public administrations is the need to integrate public health, logistics and cyber security into strategic planning, as well as to strengthen international partnerships for managing global public goods. In this sense, the pandemic was not only a crisis but also a catalyst for the transformation of security governance.

Lessons from the War in Ukraine: Energy Security, Logistics and Strategic Adaptation

Russia's full-scale invasion of Ukraine in February 2022 represented the largest conventional war on the European continent since 1945 and generated systemic effects on the Euro-Atlantic security architecture. At the same time, it provided a "laboratory" for understanding the relationship between economics and military strategy, revealing a series of **key lessons** for public administrations and international institutions (Chivvis, 2023).

Energy security is one of the central lessons. Before the invasion, Europe's dependence on Russian gas seemed manageable through long-term commercial contracts. The war demonstrated, however, that energy infrastructure can be

weaponised. Reduced deliveries of gas, attacks on critical infrastructures and price volatility prompted the European Union to accelerate plans to diversify sources, create strategic reserves and invest in renewable energy and interconnection infrastructures (European Commission, 2023). Energy security is no longer an isolated economic issue but a core component of strategic resilience and the ability to sustain a defence effort.

A second key aspect concerns **military logistics**. The war in Ukraine has shown that continuous supply of ammunition, fuel, equipment and spare parts is as important as technological superiority. Lack of logistical coordination can undermine operational advantages, while railway networks, depots and transport corridors become strategic targets. NATO and the EU have launched initiatives to improve military mobility, simplify customs procedures and modernise critical infrastructure so that troops and equipment can be moved quickly on the eastern flank (NATO, 2023b). This lesson is particularly relevant for Romania and the Baltic States, which constitute key areas for deterrence.

The third lesson involves **strategic and doctrinal adaptation**. The conflict has highlighted the role of emerging technologies, from commercial drones used for military purposes to information warfare and cyber-attacks against critical infrastructures. This obliges public administrations and armed forces to integrate technological innovation more rapidly, develop dual-use capabilities and invest in protecting the cyber domain and communications (IISS, 2023). At the same time, international cooperation in training and equipment transfer has shown that alliances can act as force multipliers when there is political will and effective coordination mechanisms.

On the economic plane, the conflict demonstrated that **financial and trade sanctions** can be used as instruments of deterrence and strategic coercion. Freezing foreign reserves, restricting technology exports and excluding Russian banks from international payment systems have undermined Moscow's ability to finance its war effort, showing that economic interdependence can be transformed from a vulnerability into a foreign-policy tool (CFR, 2022).

In conclusion, the war in Ukraine confirms that security in the twenty-first century is **multidimensional**, and the success of defence strategies depends on integrating energy, logistics, economic and technological dimensions. For public administrations in NATO and EU member states, the lessons of the war imply the need for more comprehensive planning, strengthening the resilience of critical infrastructures and accelerating investment in emerging capabilities, alongside deepening international cooperation.

Economic – Military Strategy Interdependence: Technology, Defence Industry and Digitalisation

Amid the accelerated transformations of the security environment, **the interdependence between the economy and military strategy** has become more visible than ever. On the one hand, the economy provides the resources, infrastructure and human capital necessary to build and modernise military capabilities. On the other, defence strategies and security investments generate multiplier effects on the economy, stimulating innovation, the development of critical infrastructure and the creation of jobs (Băhnăreanu, 2009).

A central domain of this interdependence is **investment in technology**. Progress in artificial intelligence, autonomous systems, advanced sensors or encrypted communications is redefining how military operations are conceived. States that invest consistently in research and development and in the technological transfer between the civil and military sectors enhance their ability to maintain a competitive edge (Gilli and Gilli, 2019). In the United States, the “*innovation ecosystem*” model has generated technology companies collaborating with the Pentagon; in Europe, the European Defence Fund supports joint research projects for emerging technologies with dual-use applications (European Commission, 2022).

The defence industry is another pillar of this relationship. It acts as an **interface between the economy and strategy**, transforming financial resources allocated to defence into equipment, services and real capabilities. A solid industrial base enables states not only to meet their own needs but also to export strategic products, thus strengthening their international influence. In the context of the war in Ukraine, the importance of secure supply chains and the ability to ramp up ammunition production became evident, prompting the European Union to adopt measures to stimulate production and coordinate joint procurement (European Defence Agency, 2023).

An emerging element of the economy – strategy interdependence is **digitalisation**. Digital technologies – big data, cloud computing, artificial intelligence – are transforming planning, command and logistics processes within defence institutions. Armed forces are investing in digital platforms for resource management, simulations and virtual exercises, while public administrations are developing dashboards and integrated systems for evaluating security policies (NATO, 2023c). This transformation is not only technical but also organisational, requiring new skills and new models of data governance.

Alongside the obvious advantages, the interdependence between the economy and military strategy also raises **challenges**. Massive investments in emerging

technologies can create critical dependencies on foreign suppliers, while the transfer of dual-use technology involves risks of proliferation and cyber security. Moreover, robust **inter-institutional coordination** is necessary to avoid duplication and to ensure the efficient use of resources. Public administrations must therefore develop support policies for the defence industries, mechanisms for information sharing and training programmes for strategic leadership and risk analysis (OECD, 2022).

In conclusion, the interdependence between the economy and military strategy is not merely a passive phenomenon but can be **actively shaped** through coherent public policies, public – private partnerships and smart investments in technology and digitalisation. Such an approach can turn defence spending from a necessary cost into a driver of innovation and national resilience, thereby consolidating security as a public good.

CONCLUSIONS AND RECOMMENDATIONS

The analysis presented in the first two chapters highlights the complex nature of security as a public good, both at the national and global level. Starting from its theoretical foundations – non-excludability, non-rivalry, the free-rider problem and the role of public policies – it becomes clear that security can no longer be approached merely as a military function of the state, but rather as a **multidimensional** ecosystem in which health, energy, cyber resilience and financial stability are essential components. Within this framework, public administration acts as the orchestrator of resources and partnerships, while international institutions such as NATO and the European Union operate as providers and coordinators of global public goods.

The practical dimension of the analysis shows that **economic resources** constitute the foundation of military power. Budget allocations for defence – exemplified by the 2% of GDP benchmark assumed within NATO – are not just accounting figures but the expression of political will and long-term security strategy. The COVID-19 pandemic demonstrated that national security is inseparable from public health and the functioning of supply chains, while the conflict in Ukraine showed that energy security and military mobility are as important as technological modernisation. Investments in industry, critical infrastructures and digitalisation can turn defence spending from a burden into a driver of innovation and economic resilience.

Based on these findings, several complementary recommendations emerge:

- **Establish a national framework for policy evaluation** in the field of defence and resilience, to monitor the impact of programmes and allow rapid

adjustments to changes in the strategic environment. Such a framework would integrate performance indicators, independent audits and public reporting, strengthening transparency and accountability of decision-makers.

- **Integrate data from NATO, SIPRI, the World Bank or Eurostat into public dashboards enabling international comparisons** and supporting evidence-based decision-making. These tools would facilitate understanding of the distribution of defence effort, spending trends and structural vulnerabilities.
- **Develop public – private partnerships for dual-use capabilities and secure supply chains.** In an interdependent economy, the private sector holds a significant share of critical infrastructures and technological know-how. Public policies should stimulate collaboration and innovation in areas such as cyber security, ammunition production, energy and communications.
- **Launch training programmes for strategic leadership, risk analysis and data governance** within public administration and the security sector. Qualified human resources are the key element that can transform financial investments into real capacity for reaction and planning.
- **Implement integrated plans for military mobility and critical infrastructure interoperable with Euro-Atlantic standards,** ensuring that crisis responses are rapid and coordinated. Lessons from the conflict in Ukraine show that transport, storage and communication infrastructure can be decisive factors in deterring aggression.

These recommendations should not be seen as isolated initiatives but as part of an **adaptive governance strategy** connecting economic, defence and social policies. A public administration oriented towards resilience, transparency and partnership can transform current challenges – pandemics, conflicts, energy crises – into opportunities for strengthening collective security. In this way, security remains a public good, but one delivered through smart public policies, international cooperation and the active involvement of all relevant actors.

BIBLIOGRAPHY:

1. Băhnăreanu, C. (2009), *The Influence of the Economic Factor in Achieving Security*. Bucharest: "Carol I" National Defence University Publishing House.
2. Born, H., Fluri, P., Johnsson, A. (2003). *Handbook on Parliamentary Oversight of the Security Sector*. Geneva: DCAF – Geneva Centre for the Democratic Control of Armed Forces.
3. Buchanan, J.M. (1965). 'An Economic Theory of Clubs', in *Economica*, vol. 32, no. 125, pp. 1-14.

4. CFR (Council on Foreign Relations) (2022). *'Sanctions on Russia: Impacts and Effectiveness'*, <https://www.cfr.org/backgrounder/sanctions-russia-ukraine-war>, retrieved on 5 September 2025.
5. Chivvis, C. (2023). *'Lessons from the Ukraine War for U.S. Strategy in Europe'*, in Foreign Policy Research Institute, March, <https://www.fpri.org/article/2023/03/lessons-from-the-ukraine-war-for-u-s-strategy-in-europe>, retrieved on 22 September 2025.
6. Dunn, W.N. (2017). *Public Policy Analysis: An Integrated Approach*. 6th edn. New York/Abingdon: Routledge.
7. ENISA (European Union Agency for Cybersecurity) (2021). *ENISA Threat Landscape 2021*, <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021>, retrieved on 2 September 2025.
8. Erste Group (2025). *'Romania: A New Era of Defense Expenditure'*, <https://www.erstegroup.com/en/research/report/en/SR436222>, retrieved on 2 September 2025.
9. EUISS (European Union Institute for Security Studies) (2021). *Pandemic geopolitics: COVID-19 and the international order*, <https://www.iss.europa.eu/content/pandemic-geopolitics-covid-19-and-international-order>, retrieved on 9 September 2025.
10. European Commission (2022). *'European Defence Fund: 61 collaborative defence research and development projects selected'*, <https://ec.europa.eu/defence-industry-space/european-defence-fund>, retrieved on 8 September 2025.
11. European Commission (2023). *'REPowerEU Plan: Affordable, Secure and Sustainable Energy for Europe'*, <https://commission.europa.eu/repower-eu-plan>, retrieved on 8 September 2025.
12. European Council (2023). *'EU support for Ukraine: military assistance and macro-financial aid'*, <https://www.consilium.europa.eu/en/policies/eu-support-ukraine/>, retrieved on 18 September 2025.
13. European Defence Agency (2023). *'Supporting Ammunition Production and Joint Procurement in the EU'*, <https://eda.europa.eu/news-and-events/news>, retrieved on 18 September 2025.
14. Gilli, A., Gilli, M. (2019). *'Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage'*, *International Security*, vol. 43, no. 3, pp. 141-189.
15. Global Firepower (GFP) (n.d.). *'2023 Military Strength Ranking'*, <http://www.globalfirepower.com/countries-listing.asp>, retrieved on 16 September 2025.
16. Government of Romania (2022). *Government Programme 2021-2024*. Chapter: Defence and Public Order. Bucharest: Government of Romania.
17. IISS (International Institute for Strategic Studies) (2023). *The Military Balance 2023*. London: Routledge.
18. Janes (2025). *'White paper assessing NATO's 5% defence spending plan'*, <https://www.janes.com/osint-insights/defence-and-national-security-analysis/nato-spending-plan-assessment-white-paper>, retrieved on 20 September 2025.
19. Kaul, I., Conceição, P., Le Goulven, K., Mendoza, R.U. (eds.) (2003). *Providing Global Public Goods: Managing Globalization*. New York: Oxford University Press.
20. Kennedy, P. (1987). *The Rise and Fall of the Great Powers: Economic Change and Military Conflict from 1500 to 2000*. New York: Random House.

21. Keohane, R.O., Nye, J.S. (2001). *Power and Interdependence*, 3rd edn. New York: Longman.
22. MoND (Ministry of National Defence – Romania) (2007-2023). '*Budget. Information regarding the Budget of the Ministry of National Defence*', <http://www.mapn.ro/buget/index.php>, retrieved on 8 September 2025.
23. MoND (Ministry of National Defence – Romania) (2021). *Report on the Involvement of the Romanian Army in Managing the COVID-19 Pandemic*. Bucharest: MoND.
24. Monitorul Apărării (2021). '*NATO report on military spending in 2020. Only 11 countries meet the recommendation to increase the defence budget*', 17 March, <https://monitorulapararii.ro/raport-nato-despre-cheltuielile-militare-in-2020-doar-11-tari-respecta-recomandarea-de-a-creste-bugetul-apararii-1-36008>, retrieved on 20 September 2025.
25. Musgrave, R.A. (1959). *The Theory of Public Finance: A Study in Public Economy*. New York: McGraw-Hill.
26. NATO (2023-a). '*Defence Expenditure of NATO Countries (2014-2023)*', https://www.nato.int/cps/en/natohq/news_220195.htm, retrieved on 14 September 2025.
27. NATO (2023-b). '*Improving NATO Military Mobility: Projects and Funding*', https://www.nato.int/cps/en/natohq/topics_152817.htm, retrieved on 14 September 2025.
28. NATO (2023-c). '*NATO Digital Transformation and Emerging Technologies*', https://www.nato.int/cps/en/natohq/topics_184303.htm, retrieved on 14 September 2025.
29. NATO (2025). '*The Hague Summit Declaration*', 25 June, https://www.nato.int/cps/en/natohq/official_texts_236705.htm, retrieved on 14 September 2025.
30. OECD (Organisation for Economic Co-operation and Development) (2020). '*COVID-19 and Global Supply Chains: Disruptions and Policy Responses*', <https://www.oecd.org/coronavirus/policy-responses/covid-19-and-global-supply-chains-disruptions-and-policy-responses>, retrieved on 18 September 2025.
31. OECD (Organisation for Economic Co-operation and Development) (2022). *Industrial Policy for the Defence Sector: Ensuring Resilient Supply Chains*. Paris: OECD.
32. Olson, M. (1965). *The Logic of Collective Action: Public Goods and the Theory of Groups*. Cambridge, MA: Harvard University Press.
33. Ostrom, E. (1990). *Governing the Commons: The Evolution of Institutions for Collective Action*. Cambridge: Cambridge University Press.
34. Romania Insider (2025). '*Romania adheres to 5%-of-GDP defence spending target*', 3 June, <https://www.romania-insider.com/romania-defence-budget-june-2025>, retrieved on 13 September 2025.
35. Rothstein, B. (2011). *The Quality of Government: Corruption, Social Trust, and Inequality in International Perspective*. Chicago: University of Chicago Press.
36. Samuelson, P.A. (1954). '*The Pure Theory of Public Expenditure*', in *The Review of Economics and Statistics*, vol. 36, no. 4, pp. 387-389.
37. SIPRI (Stockholm International Peace Research Institute) (2021). '*World Military Spending Rises to Almost \$2 Trillion in 2020*', <https://www.sipri.org/media/press-release/2021/world-military-spending-rises-almost-2-trillion-2020>, retrieved on 5 September 2025.

38. SIPRI (Stockholm International Peace Research Institute) (2023). *SIPRI Military Expenditure Database*, <https://www.sipri.org/databases/milex>, retrieved on 14 September 2025.
39. Smith, R. (2019). *Defence Economics*, 3rd edn. London: Routledge.
40. Tooze, A. (2006). *The Wages of Destruction: The Making and Breaking of the Nazi Economy*. London: Allen Lane.
41. United Nations (UN) (2004). 'A More Secure World – Our Shared Responsibility – Report of the High-level Panel on Threats, Challenges and Change', 2 December, <https://www.un.org/peacebuilding/content/more-secure-world-our-shared-responsibility-%E2%80%93-report-high-level-panel-threats-challenges-and>, retrieved on 21 September 2025.
42. WHO (World Health Organization) (2021). *World Health Statistics 2021: Monitoring Health for the SDGs*. Geneva: WHO.

APPROACHES TO THE REQUIREMENTS AND OPPORTUNITIES FOR INTEGRATING THE ROMANIAN ARMED FORCES' KEY CAPABILITIES IN ALLIED MULTI-DOMAIN OPERATIONS

Colonel Iulian-Radu MONORANU, Doctoral student

Senior instructor, "Nicolae Bălcescu" Land Forces Academy, Sibiu

DOI: 10.55535/RMT.2025.3.36

The complexity of the contemporary security environment and the realities of global strategic competition compel NATO member states to develop interoperable multi-domain capabilities capable of addressing both hybrid and conventional threats. Positioned on NATO's eastern flank and in close proximity to strategically contested areas such as the Black Sea, Romania plays a critical role in the Euro-Atlantic defensive architecture. This article explores the doctrinal foundations of Multi-Domain Operations (MDO), NATO interoperability requirements, and Romania's modernization efforts, including key acquisition programs such as Patriot, HIMARS, F-16, F-35, and unmanned aerial systems. It highlights the doctrinal, organizational, and technological challenges facing Romania's integration into allied MDO frameworks, concluding that success hinges on synchronized doctrinal reform, sustained technological investment, and enhanced joint training. Romania possesses the potential to become a significant MDO contributor, provided a coherent and sustained national approach is adopted.

Keywords: Romania; capabilities; operations; multi-domain; integration;

INTRODUCTION

The evolution of the international security environment is currently marked by a high degree of complexity, volatility, and interdependence, driven by intensified strategic competition among major powers, the proliferation of regional conflicts, and the rapid acceleration of technological progress. Within this context, Multi-Domain Operations (MDO) have emerged as a critical operational paradigm for adapting modern military structures to new types of threats. The MDO concept entails the integration and synchronization of capabilities across multiple domains - land, air, maritime, space, cyber, electromagnetic, and informational – in order to achieve decisive operational advantage. For NATO, this approach constitutes a *sine qua non* for maintaining strategic superiority and defensive cohesion along its exposed flanks. The implementation of a multi-domain operational framework has become a core objective reflected in joint doctrinal developments and consistently reaffirmed in NATO summit declarations since 2020.

Positioned on the Alliance's eastern flank, with the Black Sea representing a space of strategic interest, Romania faces a unique set of challenges and opportunities in adapting to MDO requirements. Its proximity to increasingly contested areas, particularly in the face of Russia's assertive posture, combined with the geostrategic relevance of national territory, necessitates the strengthening of national capabilities and their coherent integration into NATO's security architecture. In this regard, the Romanian Armed Forces have initiated an accelerated modernization process, including the procurement of advanced air defense systems, artillery and missile platforms, aircraft, and multi-domain compatible unmanned aerial systems – all aimed at supporting participation in joint and allied operations. However, the absence of a dedicated national doctrine for MDO, alongside budgetary and organizational constraints, remains a limiting factor in fully leveraging these capabilities.

In this context, the present article aims to analyze the doctrinal, technological, and organizational requirements for integrating the capabilities of the Romanian Armed Forces into allied Multi-Domain Operations (MDO), to assess the potential of key capabilities acquired over the past decade, and to identify strategic opportunities for strengthening interoperability with NATO. The research adopts a qualitative methodological approach designed to provide a comprehensive and structured analysis.

First, a document-based analysis of NATO's doctrinal and conceptual framework is employed to identify operational requirements and interoperability principles that shape the integration of national capabilities. Second, a comparative method is applied by examining Romania's doctrinal evolution in relation to similar experiences and approaches adopted by other allied states. Additionally, major national military modernization programs are analyzed through a case study focusing on key capabilities acquired in the past decade, in order to evaluate their compatibility with MDO requirements.

Through this methodological framework, the article seeks to offer both a theoretical foundation for understanding the issue and a practical assessment of the Romanian Armed Forces' operational realities. The research findings aim to generate practical recommendations relevant to Romania's doctrinal and institutional transformation, as well as to the strengthening of NATO's collective posture on its eastern flank and in the Black Sea region.

NATO'S DOCTRINAL FRAMEWORK AND THE REQUIREMENTS FOR MULTI-DOMAIN INTEGRATION IN THE ALLIED CONTEXT

The United States Armed Forces have emerged as the undisputed leader in the development of modern operational doctrines, leveraging extensive experience in various theatres of operations, substantial resources, and a highly advanced research and experimentation infrastructure. This capability has enabled the testing and real-world validation of innovative concepts, providing a doctrinal model of reference for Western militaries. One such example is the Multi-Domain Operations (MDO) concept, grounded in the successfully validated principles of Air Land Battle, but adapted and formulated as a response to global strategic competition and the challenges posed by actors such as Russia and China (Wille, 2019). Reinforced by the lessons learned from the Second Nagorno-Karabakh War and accelerated by the outbreak of the Russia-Ukraine conflict, MDO was formally adopted as official doctrine by the U.S. Army with the publication of the revised FM 3-0 Operations manual in October 2022 (U.S. Army, 2022). The MDO concept promotes the synchronized integration of land, air, maritime, space, cyber, and information domains to achieve decision-making and operational superiority in a complex and interdependent conflict environment.

Designing a new multi-domain operational architecture required the prioritization of next-generation capabilities, such as long-range precision strike systems, integrated air and missile defense, next-generation manned and unmanned aerial platforms, high-firepower and highly mobile armored vehicles, resilient

communication infrastructure able to function in contested and electromagnetically degraded environments, as well as enhanced soldier lethality (Roper, Grassetti, 2018). In parallel, the creation of dedicated force structures capable of employing these capabilities became another key line of effort in the implementation of the new concept. To this end, the five Multi-Domain Task Forces (MDTFs) established and equipped by the U.S. Army to date (Feickert, 2025) represent organizational structures that bring all five warfighting domains under a single command, capable of delivering synchronized effects across time and space (Borne, 2019).

The influence of Multi-Domain Operations (MDO) on NATO is deep, prompting the Alliance to recalibrate its planning processes and operational concepts in order to maintain cohesion and interoperability. As such, MDO functions not only as a U.S. doctrinal construct but also as a driver of allied transformation, steering Western forces toward an integrated, flexible, and adaptive operational model.

NATO's doctrine for joint operations, the Allied Joint Doctrine (AJP-01), updated in 2022, incorporates the multi-domain dimension as a natural extension of the joint operational concept. This development reflects the Alliance's recognition of the decisive influence of the cyber and space domains on military operations, as well as the need for their convergence with traditional domains – land, maritime, and air. Unlike the U.S. approach, NATO's vision also integrates the complementary actions of non-military actors (political, economic, industrial), which can be embedded within allied campaigns to generate converging effects (AJP-01, 2022).

The NATO Concept for Multi-Domain Operations, adopted by member states in May 2023, constitutes a foundational doctrinal pillar for the Alliance's future transformation. The document defines MDO as *"the orchestration of military and non-military activities across all domains to produce converging effects"*, and emphasizes the need to operate at *"the speed and scale of modern operations."* (NATO ACT, 2023). This orientation is designed to provide allied forces with the flexibility required to confront adversaries capable of employing hybrid strategies, anti-access/area-denial (A2/AD) capabilities, and tools of competition that operate below the threshold of armed conflict.

A report published in July 2023 by military experts and strategists from the Atlantic Council, titled *"NATO Multidomain Operations: Near- and Medium-Term Priority Initiatives"*, outlines the main directions for implementing the Allied concept of Multi-Domain Operations (MDO) at the level of NATO member states. The document also offers an assessment of the capabilities considered essential for the future conduct of MDO, based on lessons identified from the Russia-Ukraine conflict. In this regard, the report establishes a prioritization framework focused

on objectives that are feasible in the short and medium term and accessible to all allies. Specifically, the study highlights the need to achieve the following capability objectives (Kramer et al., 2023):

- the development of multi-domain surveillance networks and low-cost, integrated sensor-to-shooter systems based on unmanned aerial, land, and maritime platforms;
- the enhancement of multi-domain capabilities aimed at neutralizing enemy air defense systems;
- the integration of cyber and kinetic strike capabilities targeting adversary logistics and critical infrastructure supporting the war effort, alongside the development of robust cyber defense capabilities, both governmental and private, focused on the protection of critical military infrastructure;
- the implementation of dynamic logistical support solutions, including the use of artificial intelligence, to ensure operational sustainability during high-intensity conflicts;
- the development of multi-domain support capabilities for forward-deployed forces, aimed at increasing their survivability and lethality during the initial phases of conflict;
- the assurance of wartime access to space-based capabilities provided by the private sector, in support of NATO's Alliance Persistent Surveillance from Space (APSS) initiative;
- the establishment of Multi-Domain Task Forces (MDTFs) to coordinate and integrate available capabilities across all operational domains.

In parallel with the alignment of member states' doctrines to multi-domain principles, a second strategic priority is the acquisition and development of modern, interoperable, and complementary multi-domain capabilities that enable allied force structures to achieve information superiority and create the conditions for timely and convergent responses to adversaries' multidimensional challenges.

The successful integration of multi-domain capabilities depends on the development of resilient digital networks capable of linking sensors and engagement systems through an *"any sensor – any shooter"* model. Initiatives such as Federated Mission Networking (FMN) and Combined Joint All-Domain Command and Control (CJADC2) form the technological foundation for this interoperability, enabling rapid information sharing and decision-making at operational speed (Jaspreet, 2023).

A core requirement of the allied doctrinal framework is the ability to integrate traditional means with emerging technologies, including unmanned systems, hypersonic missiles, artificial intelligence, cloud-based data architectures,

and electromagnetic spectrum capabilities. This integration must occur not only at the technical level but also procedurally, through the adaptation of common tactics, techniques, and procedures.

The implementation of Multi-Domain Operations (MDO) undoubtedly requires a revision of allied force structures and command-and-control arrangements. Following Russia's invasion of Ukraine and the activation of NATO's Graduated Response Plans in February 2022, the Alliance adopted a new NATO Force Model, one of its key components being the Allied Reaction Force (ARF) – a multinational, multi-domain high-readiness force composed of land, air, maritime, special operations, cyber, space, logistics, and strategic communications elements (NATO. INT, 2025). This structural shift materialized through the tripling of forward-deployed forces on NATO's eastern flank. Specifically, the four original battalion-level Enhanced Forward Presence (eFP) battlegroups deployed in the Baltic States and Poland were supplemented by four additional battlegroups in Bulgaria, Hungary, Romania, and Slovakia, with plans to upgrade these to brigade level (Monaghan et al., 2024). This posture reflects the application of a key MDO doctrinal principle – *“forward positioning of calibrated force packages”* (TRADOC, 2018).

In line with the U.S. Army's restructuring of land forces into theatre – corps – division echelons, NATO may increasingly consider the creation of combined structures akin to Multi-Domain Task Forces (MDTFs), integrated into the broader allied force architecture. Such formations would offer a practical foundation for MDO implementation at the alliance level, drawing on lessons learned from the U.S. Army's second operational MDTF, already activated under U.S. European Command (EUCOM) in Wiesbaden, Germany. From the U.S. perspective, MDTFs serve as theatre-level formations centered on deep fires capabilities, strategically positioned and specifically designed to support penetration and disintegration of Anti-Access/Area Denial (A2/AD) systems. A typical MDTF structure includes a precision fires battalion, an air and missile defense battalion, a logistics support battalion, and critically, a Multi-Domain Effects Battalion (MDEB). The MDEB plays a central role through its employment of reconnaissance satellites, space-based sensors, unmanned aerial vehicles (UAVs), and radar systems, enabling the integration and analysis of multi-source intelligence. It also conducts operations designed to disrupt adversary activities using non-kinetic means such as electronic warfare, cyberattacks, and psychological operations (Ki-Chul, 2025). A possible organizational model for an MDTF assigned to a Combined Joint Task Force at the theater level is illustrated in *Figure 1*.

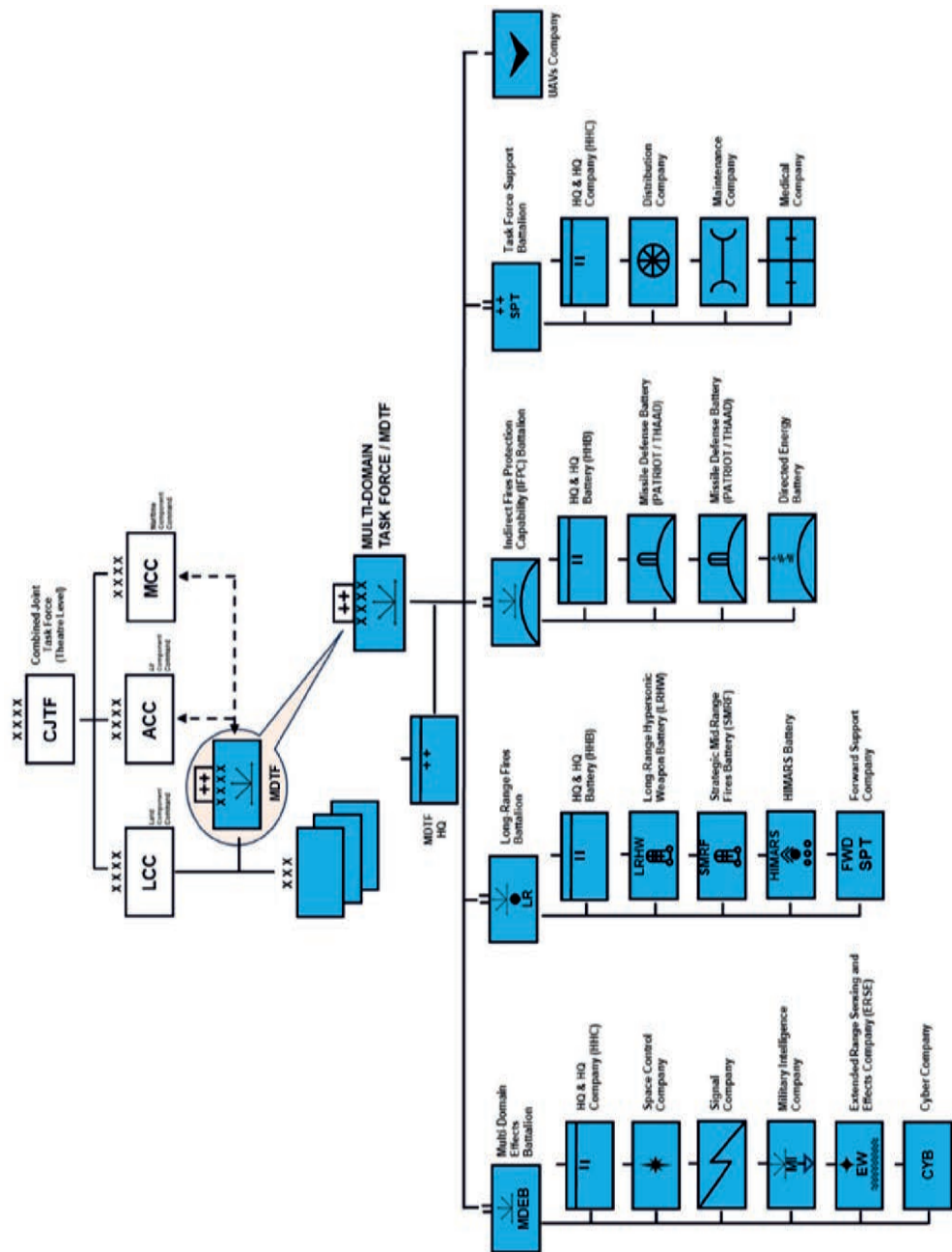


Figure 1: Organizational Model for an MDTF assigned to a Combined Joint Task Force at the Theater Level, adapted from (Higgs, 2025, p. 81)

At the allied level, NATO's efforts to operationalize MDO concept also focus on integrating multi-domain principles into planning, training, and multinational exercises, with an emphasis on preparing forces to conduct simultaneous operations across interdependent environments. Major exercises such as Trident Juncture and Steadfast Defender serve as real-world laboratories for testing these concepts and identifying interoperability gaps across nations and service branches. For example, Steadfast Defender 2024, the largest NATO exercise since the end of the Cold War, demonstrated the strength of the transatlantic bond and NATO's ability to conduct complex collective defense operations across all domains. The exercise tested the mobilization and employment of allied forces in a high-end conflict scenario, leveraging NATO, national, and multinational multi-domain capabilities across continental Europe (SHAPE, 2024).

Scientific research in the MDO domain reveals that while some NATO members possess advanced infrastructure, including integrated C4ISR systems, space capabilities, and combat-use AI, others face doctrinal, technological, or budgetary limitations. Key challenges identified include the absence of a common digital architecture among allies, difficulties integrating cyber and space capabilities into operational chains of command, and the resilience of command-and-control systems in contested environments. Moreover, recent operational challenges, particularly the war in Ukraine and conflicts in the Middle East, have accelerated efforts to effectively integrate multi-domain actions and offer critical lessons for shaping a coherent, integrated, and effective approach within contemporary allied military structures.

KEY CAPABILITIES OF THE ROMANIAN ARMED FORCES RELEVANT TO MULTI-DOMAIN OPERATIONS

The challenges and tensions generated by the increasingly aggressive actions of the Russian Federation along NATO's eastern border have prompted member states – and Romania in particular – to redefine their strategic posture for deterrence and defense. The war in Ukraine has underscored the urgent need for an accelerated doctrinal transformation of the Romanian Armed Forces to ensure alignment with the demands of high-intensity, multi-domain, and hybrid conventional warfare. This transformation seeks to shift from a predominantly reactive posture to a more proactive role within the European defense architecture by strengthening interoperability with NATO, enhancing ground mobility, air defense, and rapid reaction capabilities. In this context, Romania has intensified the military capability development process initiated in 2015, with immediate priority given to long-range

precision strike systems, air defense platforms, modern aerial assets, and new ISR (Intelligence, Surveillance, Reconnaissance) capabilities. These elements represent the core pillars of Romania's contribution to the allied defensive posture on the eastern flank.

The acquisition of High Surface-to-Air Missile (HSAM) systems – Patriot – has provided Romania with a modern and robust air and missile defense capability, fully compatible with NATO's Integrated Air and Missile Defence System (NATO IAMD). These systems are capable of simultaneously intercepting short- and medium-range ballistic missiles, cruise missiles, and combat aircraft. Their integration into the NATO defense structure enables Romania to respond promptly to Anti-Access/Area Denial (A2/AD) threats and to conduct joint air defense operations alongside allies operating the Patriot system, including the United States, Poland, Germany, the Netherlands, Italy, Spain, and Greece. The Patriot system's contribution to NATO Multi-Domain Operations (MDO) scenarios is highlighted by its role as a critical node within NATO IAMD, and by its ability to interoperate with Aegis systems, allied radar platforms, and integrated command-and-control solutions such as the Integrated Battle Command System (IBCS). Furthermore, these systems enhance the cyber and electromagnetic resilience of command architectures and support digital interoperability, including compatibility with NATO networks such as Link 16, which enable real-time target data sharing and a common operational picture of the battlespace.

Romania currently possesses 54 HIMARS (High Mobility Artillery Rocket System) launchers, organized into three battalions, each capable of launching GMLRS (Guided Multiple Launch Rocket System) munitions with a range of 70-80 km, as well as ATACMS (Army Tactical Missile System) missiles with ranges of up to 300 km. HIMARS interoperability has already been validated during U.S. and NATO multinational exercises. For example, Romanian launchers and radar systems deployed at Mihail Kogălniceanu Air Base were successfully integrated into allied C4ISR networks during the *"Arcane Thunder 23"* exercise, led by the U.S. Multi-Domain Task Force (MDTF) assigned to the European theater (Orjanu, 2023).

HIMARS has proven interoperable not only with U.S. forces, the system's primary developer and operator, but also with European allies such as the Baltic States and Poland, where it is already in use. Successfully employed in the Ukraine conflict, HIMARS demonstrated its ability to engage long-range targets with rapid, precise, and reliable fires, reinforcing NATO members' interest in adopting the system as a core capability for territorial defense support. Its relevance to MDO stems from its integration within *"sensor-to-shooter"* networks such as

the Integrated Battle Command System (IBCS) and broader allied communication and information sharing frameworks like NATO's Federated Mission Networking (FMN). These support the *"any sensor – any shooter"* principle (Richardson, 2025), enabling HIMARS to receive and integrate targeting data from a wide range of ISR sources, including drones, satellites, and ground-based sensors to coordinate land fires with air and cyber actions, thereby generating synchronized, cross-domain effects. Furthermore, the system's high mobility and survivability allow for rapid deployments and engagements from unexpected positions – critical attributes for dispersed operations and for maintaining sustained operational tempo in dynamic battlespaces.

The Romanian Air Force has made significant progress in modernizing its operational capabilities through the acquisition of three full squadrons of F-16 Fighting Falcon multirole aircraft, 48 units in total, of which 35 have already been delivered. In line with its international commitments, Romania is set to receive an additional F-16 squadron from the Royal Netherlands Air Force, following the latter's transition to the fifth-generation F-35 Lightning II platform. This acquisition is expected to bring Romania's fleet to approximately 70 modern aircraft, thereby strengthening the country's strategic relevance and deterrence posture in the regional security context. Beyond their role in NATO Air Policing, these aircraft allow for direct integration into joint aircampaigns, being interoperable with tactical data networks such as Link 16. Looking ahead, the planned procurement of 32 F-35 Lightning II aircraft, with deliveries scheduled to begin in 2030, marks the most significant step toward enhancing Romania's airpower projection capabilities. The F-35 introduces stealth characteristics, integrated sensors, and advanced data fusion, transforming it into a multi-domain network node capable of detecting, prioritizing, and transmitting target data to other allied platforms (Defense Romania, 2024). This capability enables seamless integration into allied multi-domain operations by enhancing situational awareness, survivability, and joint engagement potential across domains.

In the context of contemporary warfare, marked increasingly by the widespread use of unmanned aerial systems (UAVs), the Romanian Armed Forces have initiated a procurement program focused on Medium-Altitude Long-Endurance (MALE) platforms, while simultaneously pursuing the development of indigenous production solutions. In this regard, contracts have been signed for 7 Watchkeeper X systems (21 drones) and 6 Bayraktar TB2 systems (18 drones), most of which have already been delivered and incorporated into Romanian Land Forces units. These systems are used for reconnaissance, target acquisition, artillery and air support

coordination, and precision engagement using onboard munitions (Minculete, Păstae, 2023).

From both operational and conceptual perspectives, unmanned aerial systems contribute significantly to cross-domain synergy and the generation of high-impact, combined-action effects through the following means:

- *Dispersed ISR Sensor Networks* – UAVs enable the distribution of intelligence collection capabilities across multiple platforms and domains, offering a more complete, continuous, and disruption-resilient operational picture;
- *Integration into Multi-Domain Targeting Loops* – ISR data collected by UAVs can be rapidly integrated into command-and-fire control chains for platforms such as the F-16 or HIMARS, facilitating coordinated effects across the air, land, maritime, cyber, and electromagnetic domains;
- *Extended Surveillance Persistence* – Compared to manned aircraft, UAVs provide prolonged coverage over extended periods, enhancing the continuity of operational awareness;
- *Tactical-Level Autonomy* – Strike-capable platforms may execute rapid engagement decisions at the tactical level, reducing the need for centralized approvals where rules of engagement and C2 architectures allow;
- *Complementarity in Electronic Warfare* – UAVs can support or amplify electronic jamming, electronic intelligence, or counter-detection operations;
- *Swarm and Distributed Autonomous Operations* – UAVs may operate in coordinated formations, powered by distributed artificial intelligence algorithms, for missions such as air defense saturation, distributed ISR, or synchronized strike packages—thereby increasing operational flexibility and resilience.

The modernization of the Romanian Air Force fleet, the acquisition of HIMARS and Patriot systems, along with the strategic procurement of unmanned aerial systems (UAVs), strengthens Romania's profile as an essential operational node within NATO's multi-domain architecture. Romania actively contributes to NATO's deterrence and defense posture by deploying national forces to two of the eight Enhanced Forward Presence (eFP) battlegroups and by permanently assigning units for joint training with the eFP battlegroup stationed on its national territory. Romanian F-16 aircraft conduct airpolicing missions along NATO's eastern border, operating in coordination with aerial and airdefense systems of other member states, thereby reinforcing collective defense against threats emanating from Russia. Additionally, units from all branches of the Romanian Armed Forces regularly participate in large-scale multinational exercises, such as Defender Europe, Steadfast Defender, Dynamic Front, and Sea Shield. The Saber Guardian 25 exercise

provided Romania with the opportunity to lead, alongside U.S. forces, a multi-domain operation involving ground maneuver, river crossings, missile launches, and the validation of interoperability among command structures (MoND, 2025). Furthermore, during Steadfast Dart 2025, Romania hosted the Allied Reaction Force, a multinational formation integrating cyber and space capabilities with conventional forces, underscoring NATO's ability to conduct coordinated and effective actions in complex multi-domain operational environments (SHAPE, 2025).

Overall, the key capabilities acquired by the Romanian Armed Forces over the past decade reflect a clear trend toward alignment with Multi-Domain Operations (MDO) requirements. However, the absence of a dedicated national MDO doctrine, along with budgetary and organizational constraints, may currently limit the full exploitation of these capabilities. As a result, Romania must continue its process of doctrinal transformation and strengthen joint and allied training in order to fully harness its potential as an active contributor to NATO's multi-domain operations.

MULTIDOMAIN INTEGRATION OPPORTUNITIES AND POTENTIAL OPERATIONAL PARTNERSHIPS FOR THE ROMANIAN ARMED FORCES – A CASE STUDY

The capability portfolio previously outlined demonstrates that Romania is already aligned with NATO's requirements for operating within multi-domain architectures and can credibly integrate into dedicated allied formations, ranging from Enhanced Forward Presence (eFP) battlegroups within the Allied Reaction Force, to theatre-level Multi-Domain Task Forces (MDTFs). The decisive factor is not the isolated acquisition of platforms, but rather their integration into federated C4ISR networks capable of delivering short sensor-to-shooter loops and enabling the rapid convergence of kinetic and/or non-kinetic effects within a tactically relevant timeframe. The case study presented below will examine the main opportunities for integration, identify key NATO-compatible operational partners, outline the expected multi-domain effects, and assess the strategic relevance of Romanian capabilities in hypothetical allied MDTF scenarios.

a. The PATRIOT System – A Key Element of NATO's Integrated Air and Missile Defence System

- *Integration Opportunities:* Romania's Patriot batteries could be integrated as the air and missile defense unit within a Multi-Domain Task Force (MDTF) assigned to a Combined Joint Task Force (CJTF), connected to NATO's Integrated Air and Missile Defence (IAMD) system and, where available, to Integrated Battle Command System (IBCS) architectures.

- *Key Operational Partners:* The United States and Poland currently operate Patriot systems already integrated into emerging IBCS frameworks. Other NATO allies –Germany, the Netherlands, Italy, Spain, and Greece – also operate Patriot systems for the protection of airbases and long-range fires support units, presenting potential for enhanced interoperability.
- *Multi-Domain Effects:* Patriot batteries contribute to securing freedom of maneuver for allied ground-based missile systems, ISR platforms (manned and unmanned), and air campaigns aimed at suppressing or destroying enemy air defenses (SEAD/DEAD). This air superiority creates a time window to deliver cyber and electromagnetic effects as part of a synchronized, multi-domain offensive.
- *MDTF Integration Scenario:* Romanian Patriot systems could form the core layer of air and missile defense for a deployed MDTF, providing protection for long-range fires assets such as HIMARS launchers and artillery units, as well as for airbases from which platforms like the F-16 and, in the future, the F-35 operate.

b. HIMARS Systems in “Any Sensor – Any Shooter” Targeting Loops

- *Integration Opportunities:* Romanian HIMARS battalions or batteries could be integrated into MDTF/CJTF structures and connected to FMN, IBCS, or Link-16 networks, enabling multi-source targeting and rapid sensor-to-shooter coordination.
- *Key Operational Partners:* The United States, through the MDTF operating under EUCOM; Poland and Estonia, which currently operate HIMARS; and the United Kingdom, France, and Italy, which operate MLRS systems and possess robust ISR, electronic warfare, and cruise missile capabilities suitable for coordinated fires.
- *Multi-Domain Effects:* Interconnecting HIMARS with land-based, aerial, and space-based ISR sensors enables timely engagement of enemy command-and-control nodes, logistics infrastructure, and air defense assets, while simultaneously supporting electronic warfare and cyber effects targeting adversary networks.
- *MDTF Integration Scenario:* Romanian HIMARS systems could be employed for deep interdiction strikes against critical infrastructure and force concentrations, synchronized with aerial strikes and cyber operations, contributing directly to the disintegration of adversary A2/AD systems and enabling freedom of action for joint forces.

c. F-16 (Current) and F-35 (Future) Aircraft as MDO-Capable Air Power Vectors

- *Integration Opportunities:* Integration into combined air packages connected via NATO Link 16, enabling real-time data exchange across a broad range of weapon systems and sensors—including those of integrated air defense, artillery, and long-range strike platforms.
- *Key Operational Partners:* For F-16, partners include Poland, Greece, Turkey, and Portugal. For F-35, Romania is poised to join the global F-35 coalition alongside the United States, Italy, the United Kingdom, the Netherlands, Norway, Denmark, Belgium, Poland, Germany, and Finland, facilitating cooperative target management and interoperability in complex air operations.
- *Multi-Domain Effects:* Both F-16 and F-35 serve as central nodes for coordinating sensors, information channels, and effectors across all domains. They support real-time targeting prioritization, resource allocation, and the generation of combined and optimized effects in multi-domain operational environments.
- *MDTF Integration Scenario:* Romanian F-16s—and in the future, F-35s — could provide information superiority, designate targets for HIMARS and UAV strikes, and conduct precision strikes against adversary command centers, playing a critical role in shaping the multi-domain battlespace.

d. MALE-Class Tactical UAVs: Providing Continuous ISR and Distributed Effects

- *Integration Opportunities:* Romanian UAV detachments (Watchkeeper X, Bayraktar TB2) can be integrated into the Multi-Domain Effects Battalion of an MDTF or embedded in targeting and reconnaissance cells at brigade and division levels.
- *Key Operational Partners:* The United Kingdom (Watchkeeper), Poland and Turkey (Bayraktar TB2 and other tactical UAV families), France, Italy, and Spain (national MALE UAV programs), and the Baltic States, which operate tactical UAS and anti-UAS capabilities.
- *Multi-Domain Effects:* UAVs enable persistent ISR synchronized with HIMARS strikes and air support missions involving F-16s or F-35s. They also contribute to UAS swarming, electronic reconnaissance, and counter-UAV operations in coordination with air and missile defense systems.
- *MDTF Integration Scenario:* Romanian Army UAVs could be integrated into the Multi-Domain Effects Battalion of an MDTF for ISR missions, coordinated target engagement with missile batteries, or direct involvement in “any

sensor – any shooter” loops – for example, UAVs identify and track mobile targets, HIMARS executes precision strikes, and Patriot systems secure freedom of action against aerial threats.

With the introduction of these newly acquired systems, the Romanian Armed Forces are shaping a set of capabilities that are increasingly aligned with the standards required for integration into an allied multi-domain architecture. For instance, one can reasonably assess that an allied MDTF deployed in the Black Sea region could benefit from Romanian HIMARS for deep interdiction, Patriot systems for air and missile defense, F-16/F-35 aircraft for synchronized air campaigns, and UAVs for ISR and precision strikes – all supported by national and allied cyber and communications capabilities. A hypothetical scenario illustrating the integration of these key Romanian capabilities into a multi-domain force structure under a Combined Joint Task Force (CJTF) is presented in *Figure 2*.

The analysis indicates that Romania can position itself at the core of NATO’s multi-domain mechanisms, not merely through its inventory of platforms, but through clearly defined roles within combined force packages – such as providing air and missile defense coverage for forward-deployed units, operating long-range artillery and missile systems integrated with multi-source sensors, enabling centralized coordination with aerial platforms (particularly in the future with the F-35), and delivering persistent ISR through UAV systems. Strategic convergence with allies such as the United States, Poland, Germany, the Netherlands, Italy, the United Kingdom, France, the Baltic States, and Turkey would enable the formation of flexible, multinational, and multi-domain battle groups under a potential Combined Joint Task Force (CJTF) structure, capable of delivering decisive effects on NATO’s eastern flank. The key to transitioning from potential to operational performance lies in the institutionalization of interoperability and the regular rehearsal of multi-domain procedures within realistic scenarios alongside these strategic partners.

CONCLUSIONS

Although Romania has made significant progress in its military modernization efforts, the integration of key capabilities into NATO’s multi-domain architecture is accompanied by doctrinal, organizational, technological, and logistical challenges.

At present, the Romanian Armed Forces lack a dedicated national doctrinal framework explicitly regulating participation in multi-domain operations (MDO). In the absence of such a doctrine, adaptation relies on borrowing elements from NATO’s conceptual documents and on the experience gained through multinational exercises. This situation limits the coherence of national actions and may generate gaps between NATO requirements and Romanian operational practices.

Approaches to the Requirements and Opportunities for Integrating
the Romanian Armed Forces' Key Capabilities in Allied Multi-Domain Operations

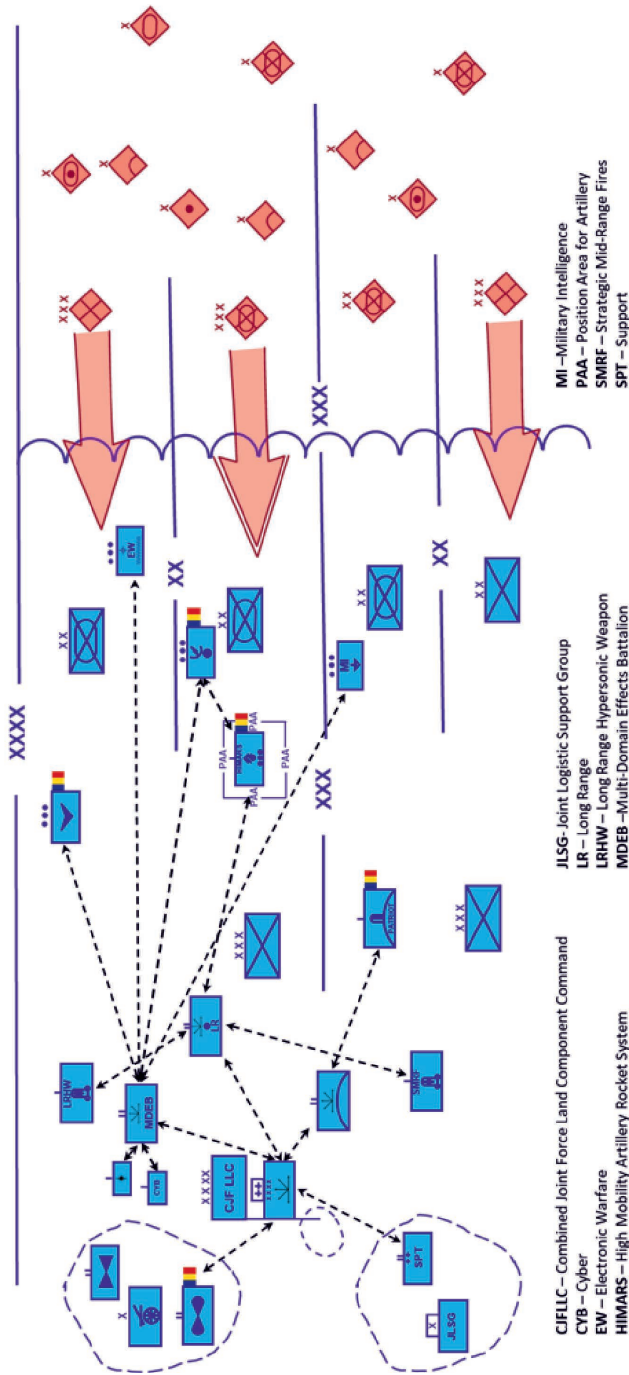


Figure 2: Hypothetical Scenario for the Integration of Key Romanian Armed Forces Capabilities into a Potential MDTF Structure within a Combined Joint Task Force (Author's Concept)

The integration of the analyzed capabilities into NATO's multi-domain networks requires full compatibility in terms of communications, data sharing, and command-and-control processes – all of which demand further technical standardization and additional investments. Budgetary constraints, training shortfalls, and personnel shortages affect the effective employment of new technologies. For example, the integration of UAVs necessitates adjustments in command structures, crew training, and organizational culture. Like wise, the transition to F-35 aircraft involves dedicated infrastructure, tailored logistics, and high operational costs, which may pose short- and medium-term obstacles.

Recent exercises and conflicts demonstrate that the success of Multi-Domain Operations (MDO) depends heavily on the protection of critical command, communications, and logistics infrastructure. In this regard, Romania faces persistent vulnerabilities in ensuring the cyber and electromagnetic resilience of its military networks. Cyber attacks and electronic jamming can degrade the effectiveness of integrated systems, significantly reducing their value in high-intensity operational scenarios.

In conclusion, Romania possesses capabilities that are largely aligned with NATO's requirements for MDO. However, the full exploitation of these assets is contingent upon addressing a series of structural and doctrinal vulnerabilities. Strengthening technical interoperability, developing a national MDO doctrine, enhancing resilience in the cyber and electromagnetic domains, and investing in joint and combined training are indispensable steps for transforming Romania's existing capabilities into decisive contributions within NATO's multi-domain operational architecture.

BIBLIOGRAPHY:

1. AJP-01. (2022). *Allied Joint Doctrine*. Bruxelles: NATO Standardization Office.
2. Borne, D. (2019). *Targeting in Multi-Domain Operations*. *Military Review*, pp. 60-67.
3. Defense Romania (2024). *Defense Romania, România a semnat contractul pentru achiziția celor 32 de avioane F-35. Forțele Aeriene Române vor consolida semnificativ capacitățile de descurajare ale NATO*. Defense Romania, https://www.defenseromania.ro/f-35-pentru-romania-dar-avioane-noi-si-in-cea-mai-moderna-versiune-pilotii-nostri-vor-zbura-pe-f-35-block-4-versiune-inca-in-dezvoltare_631591.html, retrieved on 6 June 2025.
4. Feickert, A. (2025). *The Army's Multi-Domain Task Force (MDTF)*, Congressional Research Service: <https://www.congress.gov/crs-product/IF11797>, retrieved on 6 August 2025.
5. Higgs, S.C. (2025). *Authorities and the Multidomain Task Force Enabling Strategic Effect*, in *Military Review*, pp. 78-86, <https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/March-April-2025/Multidomain-Task-Force/>, retrieved on 30 July 2025.
6. Jaspreet, G. (2023). *Return of CJADC2: DoD officially moves ahead with 'combined' JADC2 in a rebrand focusing on partners*. Breaking Defense: <https://breakingdefense.com>.

- com/2023/05/return-of-cjadc2-dod-officially-moves-ahead-with-combined-jadc2-in-a-rebrand-focusing-on-partners/, retrieved on 12 June 2025.
7. Ki-Chul, P. (2025). *How a Multi-Domain Command in Japan Would Reshape US Alliances in the Indo-Pacific*. The Diplomat: <https://thediplomat.com/2025/08/how-a-multi-domain-command-in-japan-would-reshape-us-alliances-in-the-indo-pacific/>, retrieved on 4 August 2025.
8. Kramer, F. et al (2023). *NATO Multidomain Operations: Near- And Medium-Term Priority Initiatives*. Atlantic Council. Washington, DC, USA: The Scowcroft Center for Strategy and Security.
9. MApN (2025). *Exercițiul multinațional SABER GUARDIAN 25*. Defense.ro: <https://www.defense.ro/exercitiul-multinational-saber-guardian-25>, retrieved on 23 May 2025.
10. Minculete, G., Păstae, V. (2023). *Essential approaches to combat the use of drones. Specific elements of the armed conflict in Ukraine*. Bulletin of "Carol I" National Defence University, pp. 201-211.
11. Monaghan, S. et al (2024). *Understanding NATO's Concept for Deterrence and Defense of the Euro-Atlantic Area*. Center for Strategic and Budgetary Assessments, <https://csbaonline.org/research/publications/understanding-natos-concept-for-deterrence-and-defense-of-the-euro-atlantic-area/publication/1>, retrieved on 31 May 2025.
12. NATO ACT (2023). *NATO Multi-Domain Operation Conference 2023 Raport*, www.act.nato.int: www.act.nato.int/wp-content/uploads/2024/05/2024-MDO-Catalogue-April-12.pdf, retrieved on 27 November 2024.
13. NATO.INT (2025). *NATO Force Model*, Nato.int: https://www.nato.int/cps/en/natohq/topics_234075.html, retrieved on 30 July 2025.
14. Orjanu, G. (2023). *Exercițiu militar de amploare, pe teritoriul Poloniei, României și Germaniei. "Arcane Thunder 23" ajunge și la Mihail Kogălniceanu*. Defense Romania: https://www.defenseromania.ro/exercitiul-militar-arcane-thunder-23--pe-teritoriul-poloniei--romaniei-si-germaniei_624199.html, retrieved on 8 August 2025.
15. Richardson, D. (2025). *Defending the skies – US style*. European Security & Defence, <https://euro-sd.com/2025/02/articles/42609/defending-the-skies-us-style/>, retrieved on 30 May 2025.
16. Roper, D., Grassetti, J. (2018). *Seizing the High Ground – United States Army Futures Command*. The Association of the United States Army: <https://www.ausa.org/sites/default/files/publications/SL-18-4-Seizing-the-High-Ground-United-States-Army-Futures-Command.pdf>, retrieved on 14 July 2025.
17. SHAPE (2024). *NATO wraps up Steadfast Defender 24*. <https://shape.nato.int/stde24/newsroom/news/-nato-wraps-up-steadfast-defender-24>, retrieved on 23 March 2025.
18. SHAPE (2025). *STEADFAST DART 2025*. Shape.Nato: <https://shape.nato.int/steadfast-dart>, retrieved on 11 July 2025.
19. TRADOC (2018). *Pamphlet 525-3-1, The U.S Army in Multi-Domain Operations 2028*. U.S. Army Training and Doctrine Command. Virginia, USA: United States Army Training and Doctrine Command.
20. US Army (2022). *FM 3-0 Operations*. Washington, DC: Headquarters Department of the Army.
21. Wille, D. (2019). *The Army and Multi-Domain Operations: Moving Beyond Air Land Battle*. New America: <https://www.newamerica.org/future-security/reports/army-and-multi-domain-operations-moving-beyond-airland-battle/>, retrieved on 18 June 2025.

USING THE REARM EUROPE PROGRAM TO FINANCE EUROPEAN STATES. – CASE STUDY: THE USE OF THE SAFE INSTRUMENT IN ROMANIA –

Associate Professor Dr. Vlad Ionuț DUMITRACHE

*Regional Department for Defence Resources Management Studies, Braşov;
National Defence University “Carol I”, Bucharest*

DOI: 10.55535/RMT.2025.3.37

The current European Union driven proposal of redistributing European capital to defense spending creates a unique opportunity for EU member states. While the major focus becomes how to manage national defense industries around the European continent, more funds for defense also means a readjustment for defense planning and national defense programs. In other words, the desire to rearm Europe becomes the biggest trigger for defense resources management since the Wales Summit in 2014 that enabled countries that were NATO members to enhance their defense spending percentage of the GDP to 2%. What do these increased allocations also mean in terms of NATO defense planning?

The aim of this paper is to observe through an empirical analysis the effects of using reimbursement loans that the European Union is willing to offer in order to finance defense policies in European member states. In this case particularly, the analysis will focus on consequences and effects for the Romanian state.

Keywords: defense industry; defense resources management; defense allocation; defense expenditures; defense planning;

INTRODUCTION

The invasion of Ukraine by the Russian Federation in February 2022 changed the dynamics of defense management for the states on the Eastern Flank. The focus of defense investment does no longer priorities only direct acquisitions, but also indirect investments, in transport infrastructure, in the modernization of the response capacity of institutions with a role in crisis situations, as well as in the long-term restart and reorganization of the defense industry.

The current motivation for attracting investments in defense and security areas at the European level stems from a concern of the European Union regarding a potential scenario, in which in the event of attacks launched by the Russian Federation in the European space, EU states would not immediately or in a time-effective manner benefit from aid from the United States of America, the largest NATO contributor. Over time, the amounts allocated by the US for Euro-Atlantic defense have overwhelmingly exceeded the budgetary contribution of the other member states. Thus, in 2024, the United States contributed 968 billion to the NATO budget, more than two-thirds of the budget of all other states. Germany contributed 98 billion, Great Britain 82 billion, France 64 billion, Poland 35 billion and Italy 34 billion (Mc Gerty, 2025). The large role of the United States can also be observed in the area of capabilities involved in the NATO planning process.

The European Union has begun to consider defense a priority, ever since 2016, when the first Common Security and Defense Policy of the European Union (CSDP) was developed, also following the invasion of the Russian Federation, two years earlier, in 2014, in Crimea. The war in Ukraine demonstrated the need for modern, innovative military equipment, for a developed logistics chain and for a defense industry that can supply any defense mission in the European space (Fiott, 2020). In this context, after multiple analyses, a significant gap was found between what the member states should be able to offer in terms of defense resources and what actually existed in reality at national defense levels for most EU states.

Following these observations, the need for a rearmament plan for the European Union was founded, a plan that has taken the form of ReArm Europe. Following the Munich Conference in February 2025, the European Commission analyzed the opportunity to increase the defense autonomy of the member states through increased investments in the defense industry (Wolff, 2025).

In regards to the chosen methodology for this paper, a Case Study concerning a quantitative empirical analysis will be used in order to better understand the effects of using European funds in order to fund defense related projects and programs.

THE SAFE INSTRUMENT, PART OF THE REARM EUROPE PROGRAMME

Through ReArm Europe, a military acquisition and development project that should end in 2030, the aim has become to narrow the gap between the needs of a modern and robust defense at European level and what physically exists in 2025 within the European armed forces. At the time of the decision to initiate the respective investment project, various criticisms have emerged regarding the possibility of a lack of finality in terms of the direct result and measurable objectives.

The ReArm Europe rearmament plan, through its various instruments, will bring 800 billion euros in terms of expenditures to the EU Member States. Of these funds, 150 billion (in Euro currency) will be provided through a loan through the financial instrument called SAFE (Security Action for Europe). This new financing project attracts both supporters and critics. Since 2016, when defense policy became a constant for the European Union, ReArm Europe and SAFE have come to represent by far the largest initiative to finance the defense at European level, through concrete projects with a clear destination, namely military acquisitions using the European defense industry.

On the other hand, there are experts who support the need for an international bank, which, similarly to the European Bank for Reconstruction and Development, could support long-term financing of defense investments, thus offsetting short- and medium-term loan instruments of the SAFE type. Such a proposal is represented by a possible *Rearmament Bank* (European Parliament-Briefing, 2025). Another financing option that could work is through grants, mechanisms that already operate at the European Union level for other investment programs and that do not have to be reimbursed, as it will happen in the case of the SAFE instrument.

A second concern is related to the opportunity cost of such investments. The European Union had set other priorities in previous budgets, especially in the area of green economic development, the fight against environmental and climate issues, etc. Thus, part of the European political spectrum wanted these defense investments not to affect the cohesion funds that were already allocated to other prioritized expenditures. The majority decision, however, has been to pursue the financing of the defense spectrum, with the investments to be returned

to the European economy by strictly using all European funds for acquisitions from the European defense industry. This factor, added to the growing aggressiveness of the Russian Federation on the border of the European Union, as well as a desire for European autonomy in defense issues, led to the approval of the entire ReArm Europe program. Even if the European Union wants to increase its autonomy, collaboration with NATO will continue. Recently, new defense capabilities have been proposed within the alliance, namely European Sentry, for better protection of the Eastern Flank, a capability that can also be fulfilled by the contribution of European states with equipment purchased through the SAFE financial instruments.

It should also be noted that unlike NATO funds, where various budgets can be allocated for direct operational missions, as described in the NATO Defense Plan Process (NDPP), the European Union will not allow direct finance of any type of mission or operation or developments of capabilities through the SAFE mechanism. The funds will be used strictly for weapons and equipment acquisition as well as the development of the defense industry, with the main aim of allocating financial resources on two levels:

- Restocking of ammunition, projectiles, missiles, artillery systems,
- Modern defense systems including aerial and underwater drones, artificial intelligence and other devices that contribute to electronic warfare.

In addition to these investments in equipment that may have direct objectives in the field of defense, there is also a third dimension of investment, an indirect one, linked to the broader objective of military mobility in the European space, where the need to develop new road, rail, maritime transport routes is an urgent one, especially in Eastern Europe.

Unlike other funds allocated for defense, implemented over time by the European Defense Agency, such as PESCO, the great advantages of the SAFE program relate to the guarantee of the European Union community funds, as well as a low interest rate, equal for all states that will allocate budgets by using the respective financial instrument. Another advantage is represented by the long time frame regarding the reimbursement, if the funds will be allocated in the next 5 years, the grace period is up to 10 years, the payment of the obtained loans thus starting in 2035.

Another aspect to be taken into account is that there are European Union states that are not NATO members and that can therefore contribute from a different perspective both to European collective defense and to their own national defense policies by using these newly founded instruments. One such example is Cyprus, an EU and non-NATO member state that has requested funds through the SAFE program to increase its own defense capacity.

In order to speed up the process of European rearmament, each member state has already submitted a request for funding, the individual allocation has been established and quantified according to the following *table 1*:

Table 1: How the SAFE program has been allocated between member states
(The Council of the EU, 2025)

Member State	Sum of money allocated to EU member states
Poland	43.734.100.805
Romania	16.680.055.394
Hungary	16.216.720.524
France	16.216.720.524
Italy	14.900.000.000
Belgium	8.340.027.698
Lithuania	6.375.487.840
Portugal	5.841.179.332
Latvia	5.680.431.322
Bulgaria	3.261.700.000
Eastland	2.660.932.171
Slovakia	2.316.674.361
Czech republic	2.060.000.000
Croatia	1.700.000.000
Cyprus	1.181.503.924
Finland	1.000.000.000
Spain	1.000.000.000
Greece	787.669.283
Denmark	46.796.822

Table 1 presents those states that have already requested funds through the SAFE program. States such as Germany are missing, because they did not want to access such funds for the time being, for defense purposes.

The next step is to synchronize the allocated expenditures, the budgetary destination and the internal planning documents of each member state, following which, at the end of this process, at the beginning of 2026, the European Union Council can approve the implementation plan of the entire allocation of funds.

USE OF THE SAFE INSTRUMENT IN ROMANIA

In the case of Romania, as it can be seen from *Figure 1*, the position of the state in relation to the correlation between the geographical proximity to the Russian Federation and the level of defense investment is of major importance.

Romania is rather in an area with states such as Denmark, Norway, Sweden, which are geographically further away from the Russian Federation. The same is the case with other states on the Eastern Flank such as Bulgaria and Hungary. Of the states within a 1,000 km radius of Moscow, Poland has the highest level of defense investment, with a percentage of GDP allocated to defense of over 4%.

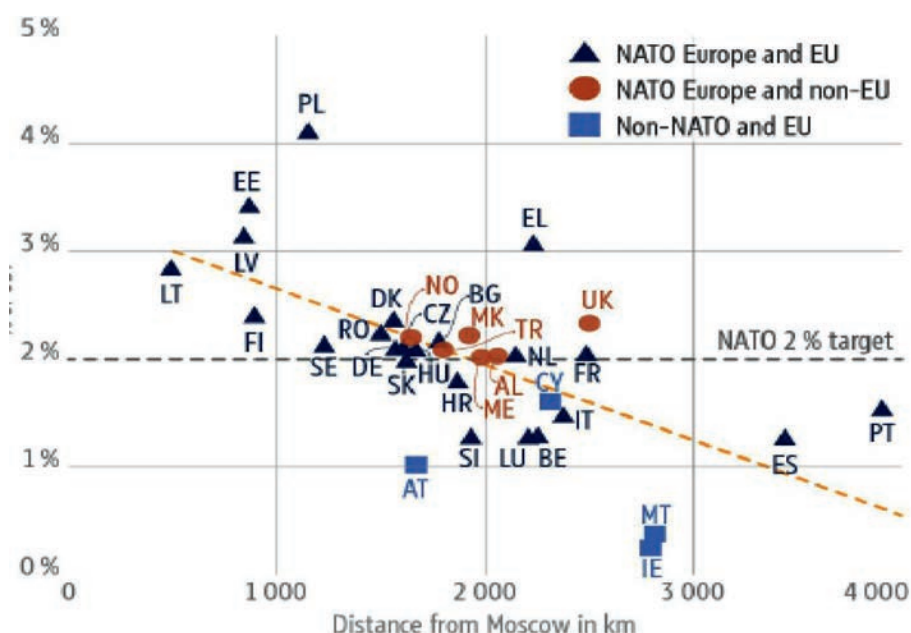


Figure 1: Defense expenditures as part of the GDP and distance from the Russian Federation for different states
 (European Parliament, 2025)

A constant problem in the case of defense investments remains the ratio between foreign acquisitions and national production. Since 2016, Romania's capacity to attract defense investments has increased, along with the percentage allocated for spending in that area, to 2% of GDP. However, most of the acquisitions have meant the imports of weapons. In current public contracts, an important part remains the Offset part (Macsim, 2024), namely the partial production of imported equipment in the country where the equipment will be used. However, in percentage terms, the Romanian arms industry has not grown in terms of turnover in an exponential way in the last 8 years (Mănescu, 2024).

A key component, which should become a priority through the new SAFE program, references to the possibility of correlating the growing investments with the development of the defense industry in Romania. This is currently happening through foreign capital, through foreign direct investments, either of the Greenfield type or acquisitions from major companies from the EU or NATO that buy out the local market. There is an enormous potential in the national defense industry of Romania, one that has existing since the communist period, and which has begun to modernize in the last decade through recalibrations, refurbishments and development of new production units. All of these aspects as well as the more recent development of the internal factor of production through FDI can be seen in *Figure 2*.



Figure 2: Defense production factories in Romania (Euromaidan Press, 2025)

For Romania, the stake was a fair allocation, which could support all European directives regarding the revitalization of the defense industry, the increase of military mobility, but also the fulfillment of the acquisition plan in accordance with its own national objectives, as they are described in the internal military planning documents. Romania has understood the major role it has in the current context, in terms of its geographic location, close to the open war front in Ukraine. Even if the funds allocated to Romania could have been even higher, somewhere around 20-25 billion EURO, the total allocation for Romania, Hungary and Poland represents half of the total amount allocated by the EU through the SAFE instrument.

The technical negotiations for what this allocation will mean should take into account several priorities. The Romanian state has an aging defense industry, whose status has been under debate for almost a decade, between remaining on the free market, at the Ministry of Economy or returning to the Ministry of Defense, where it could be subject to economic protection measures and integrated into the broader process of defense resources management.

There will be three allocation directions for the funds coming from the SAFE program. First, the process of military acquisitions will be largely increased. As seen in *Figure 2*, the priority should be an integrated acquisition process, in which the share of own production increases, possibly by developing regional hubs for domestic production and distribution/exports. This direction does not only have the economic purpose of developing certain sectors of the Romanian state on a regional and national level, but also has a strategic component, every state being in need to be able to produce military equipment on its own, in case it finds itself in a situation of armed conflict. One must not forget the difference between economy under peace terms and in war time.

The second component is the integration of a joint European effort, for many of the military capabilities that the Romanian army has planned, includes equipment produced in the European space. This approach will also involve using the local industry, be it with national capital or through foreign direct investments.

The third component can be considered the most important priority for the Romanian state, namely the indirect investments in civil infrastructure, necessary to ensure that key aspect of military mobility. The Romanian state has not managed to ensure the full development of the A7 and A8 motorways, initially financed through other European mechanisms, such as the PNRR. Now the missing sectors are going to be financed through the SAFE program, because both motorways have a strategic role, not just an economic one. The Constanța harbor is in the same strategic plan, with a vital role for the military mobility process. The development of the harbor has seen a lot of delays during the last decade. The inclusion of this objective in the SAFE financing plan thus becomes a chance for developing a strategic hub near the Black Sea. By the time this article is published, it is estimated that almost a third of the entire amount allocated to the Romanian state through the SAFE program will be distributed to the infrastructure part of the development plan (Voiculescu, 2025).

In regards to the actual financing mechanism of the SAFE program, the funds will be adopted and spent by the end of 2030, and will subsequently be reimbursed by the member states starting with 2035, in a gradual given time frame, until 2065.

All states, regardless of the amount of money received, will have to respect this schedule, including Romania.

The amount of 16 billion is a large one, but if we observe *Figure 1*, it does not represent an expenditure justified by the geographical proximity/investment level ratio. Romania has the same funds as France, located much further from the front, and Hungary, which although geographically closer to the Russian Federation is a smaller state than Romania in terms of total area and, unlike Romania, does not have an area of potential direct impact in relation to the current front, namely the Black Sea. Moreover, it can be observed that in the logic of the needs in Table 1, Poland has been allocated an amount from the SAFE program of 40 billion euros, almost triple the amount allocated to Romania. Therefore, the problem of an allocation deficiency on the South-Eastern Flank, as defined by NATO, and the North-Eastern Flank can be raised. Another problem relates to the essence of the allocation of defense funds from the SAFE program. This program represents a loan agreement, which will be repaid in 2035, at an advantageous interest rate of 3%. However, the Romanian authorities announce that they will freeze the allocation of GDP to 2.3% for defense, having the alternative of SAFE funds for large arms purchases. However, the allocations from GDP do not represent loans that must be repaid, but at the same time the Romanian state is under budgetary pressure, due to a large deficit and rising loan interest rates. In these conditions, a question arises regarding long-term projections, regarding

The expenditures are represented by long-term loans, with low interest rates, set up at maximum 3%, with a return period of ten years. If for the Romanian state, the alternative of increasing defense spending may seem complicated due to the increased deficit, another directive of the European Commission should be mentioned, which establishes that for those states that manage to reduce the deficit below a certain threshold, defense spending will subsequently be recorded separately, no longer being taken into account in the deficit calculations, thus decreasing the interest rates at which the respective state will be able to lend further funds (Council of the European Union, 2025).

CONCLUSIONS

If at European level there are several questions regarding possible negative scenarios due to the allocation of this instrument at the level of the entire continent, there are also a series of risks that must be taken into account at domestic level.

A first aspect is related to the coordination between defense planning and the actual procurement process, taking into account possible specific requirements,

production delays, synchronization with other national ministries, with the European Union bureaucracy and so on.

The Romanian state has encountered difficulties in the past in absorbing European funds, most recently in the case of the PNRR program, therefore, a source of concern may come from the lack of an effective absorption capacity of the funds allocated through the SAFE program, considering the amount of almost 17 billion that should be accessed by 2030. The administrative capacity of the Romanian state must be improved in order to not repeat past failures and in order not to fail to achieve an absorption as close as possible to 100%. The increase in the number of projects in cooperation with other member states and with industries from these states will demand a whole series of negotiations and compromises. In the past, in offset contracts, the Romanian state did not always obtain the best advantages, there have been examples with penalties and the cancelation of some contracts, examples that should be analyzed and avoided in future collaborations. It is also expected that due to the increase in demand for military equipment, due to the complicated geo-political situation, there will be delays and extended deadlines for receiving some of that specific military equipment. Under these conditions, multiple reception deadlines will be extended beyond the initial date. It will therefore be a test for the Romanian state to support an effort in the hybrid war that will be triggered by disinformation by foreign state actors. Such actions will challenge the acquisition process developed in the defense and security area. In this logic, with the increase in the number of investments, *the guns and butter effect* will also appear in the national public space, namely the analysis of that opportunity cost according to which, once important expenditures are allocated for defense, they cannot be allocated for other public needs.

A final major risk that should be taken into consideration is in another area of impact, namely the strategic and political one. There will be multiple factors to consider when such issues appear like: technology transfer, foreign suppliers, components that might not be from the European Union or even what the safe states to establish economic relations in the defense area will be. Romania's agenda and plan regarding the relationship with the United States of America and its defense industry will also remain an important factor to handle.

At external level, regarding other geopolitical factors, an increase in Romania's defense capacity, especially in terms of capabilities around the Black Sea might attract the attention of the Russian Federation, therefore the level of deterrence will have to be credible and effective, in the face of any potential threats of escalation.

However, these risks must not cancel the multiple advantages offered by the European rearmament project, started through the SAFE instrument. The massive funding, even if it could have been even greater, represents a unique opportunity for the Romanian state to reduce deficiencies in the field of defense, to modernize the armed forces, infrastructure, and mobility capacity and implicitly to develop a defense industry, which has not been a priority in the last 30 years. Romania's defense posture has the chance to evolve in accordance with the military objectives planned in the next 5 years. A possible relaxation of the budgetary pressure by reallocating defense spending through European funds will also mean reducing any risk that those planned objectives will not be obtained on time in alignment with all the military planned documents.

BIBLIOGRAPHY:

1. Bouabdallah, O., Dorrucchi, E., Nerlich, C., Nickel C., Vlad, A. (2025). *Time to be strategic: how public money could power Europe's green, digital and defence transitions*. The European Central Bank Blog.
2. Clapp, S., Delivorias, A., Lazarou, E., Pari, M. (2024). *Financing the European defence industry*. EPRS, European Parliament
3. European Parliament (2025). *ReArm Europe Plan/Readiness 2030*, Briefing, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769566/EPRS_BRI\(2025\)769566_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769566/EPRS_BRI(2025)769566_EN.pdf), retrieved on 22 August 2025.
4. Fiott, D. (2020). *The CSDP in 2020-The EU's legacy and ambition in security and defense*, European Union Institute for Security Studies.
5. Lazarou, E. (2024). *White paper on the future of European defence*. EPRS, European Parliament.
6. de Lemos Peixoto, S., Loi, G., Mazzocchi, R., Stieber, H., Sabol, M. (2025). *Defence financing and spending under the Economic Governance Framework, Economic Governance and EMU Scrutiny Unit*. European Parliament.
7. Macsim, M. (2024). *The trials and tribulations of the new offset legislation in Romania*, in *Business Review*.
8. Mănescu, G., Iancu, D. (2024). *Relevanța strategică a industriei naționale de apărare în principalele documente de planificare a apărării – o abordare contextuală, în Gândirea militară românească*
9. McGerty, F. (2025). *Global defence spending soars to new high*. International Institute for Strategic Studies, Military Balance Blog.
10. Prysiazhniuk, M., (2025), *Romania is quietly becoming Europe's defense powerhouse*, Euromaidan Press
11. The Council of the EU (2025-1). *Council activates flexibility in EU fiscal rules for 15 memberstates to increase defence spending*, Press Release, <https://www.consilium.europa.eu/en/press/press-releases/2025/07/08/council-activates-flexibility-in-eu-fiscal-rules-for-15-member-states-to-increase-defence-spending/>, retrieved on 22 August 2025.

12. The Council of the EU (2025-2): Safe Council adopts 150 billion boost for joint procurement on European security and defence, <https://www.consilium.europa.eu/ro/press/press-releases/2025/05/27/safe-council-adopts-150-billion-boost-for-joint-procurement-on-european-security-and-defence/>, retrieved on 2 August 2025.
13. Vedby Rasmussen, M. (2024). *Rearmament with a purpose*, EconPol Forum.
14. Voiculescu, L. (2025). *Cum vor fi folosiți cei 16,7 miliarde de euro din SAFE, Republica*.
15. Wolf, G., Steinbach, A., Zettelmeyer, J. (2025). *The governance and funding of European rearmament*, in *Policy Brief*, Issue no 15/25, Bruegel.

SHAPING MODERN AVIATORS: FROM TECHNICAL MASTERY TO ETHICAL LEADERSHIP

Captain Assistant Professor George-Adrian AIONESEI, Doctoral student

Lieutenant Colonel Associate Professor Dr. Cristian DRAGOMIR

"Henri Coandă" Air Force Academy, Braşov

DOI: 10.55535/RMT.2025.3.38

In aviation, the flight instructor has a central role in the pilot training process, going beyond the mere transmission of technical and fundamental knowledge to the point of engaging in shaping character, attitudes, and safety culture. In this process, the instructor has to be involved in every aspect of the pupils' development. Therefore, this article explores the complexity of the instructor's roles, such as mentor, leader, teacher, moral evaluator, coach, psychologist, innovator, and risk manager, analyzing how each contributes to the development of modern pilots.

Based on specialized literature and current needs, we propose a hierarchical conceptual model that integrates all these roles and offers a different perspective on training. By writing this article, we aim to synthesize a theoretical and practical framework for an optimal model of a flight instructor, capable of meeting current demands of global aviation.

Keywords: flight instructor; aviation; students; pilot; leader;

INTRODUCTION

The professional training of a pilot in modern times is a complex process that goes beyond the mere accumulation of theoretical and practical technical knowledge. Contemporary aviation is defined by extensive automation, integrated flight management systems, rigorous safety measures and a constant need for adaptability to unpredictable operational scenarios. In this context, the flight instructor becomes not just a transmitter of technical knowledge, but also developer of non-technical competencies, a promoter of critical thinking, and a strong advocate for safety culture. Their role is fundamental in bridging theory and real-world practice, forming a link between necessary skills required to operate an aircraft and the behaviors and attitudes essential in a complex and dynamic environment. This is also the reason why, within our scientific approach to highlighting this role, we relied predominantly, as research methods, on theoretical analysis and the comparative study of existing specialized works in the aviation field, with impact within the study of pilot training.

According to International Civil Aviation Organization – ICAO (ICAO 2013, I-3-8), the quality of training, both in the initial and recurrent phase, determines an individual's level of performance and operational resilience. ICAO doc 9995 emphasizes that pilot training should be competency-centered (Competency-Based Training and Assessment – CBTA), focusing on development of cognitive, emotional and decision-making competencies. European Union Aviation Safety Agency – EASA and Federal Aviation Administration – FAA, uphold the same standards, arguing that the mere transmission of knowledge or the reproducing standard procedures is no longer effective and sufficient. Instructor must encourage critical thinking, analyze errors and behavior adaptability in different complex and unforeseen scenarios (EASA, Easy Access Rules for Flight Crew Licencing 2020, pp. 882-884; FAA, Aviation's Instructor Handbook - FAA-H-8083-9B 2020, Ch.7, pp. 4-8).

An important aspect frequently addressed in the literature is the non-technical element of pilot training. Studies such as those by Salas et al. (Salas, Tannenbaum, et al. 2012, pp. 84-87) show that abilities like CRM (Crew Resource Management), situational awareness and stress management are responsible for more than 70% of operational success in aeronautical activities. These abilities cannot be developed

exclusively through individual study, rather, they require guidance, mentoring and continuous feedback from an experienced instructor. Therefore, the flight instructor becomes an essential part in shaping the attitude and behavior of the trainees, serving as the student pilot's first real example in handling pressure, communication and operational safety management.

Furthermore, there is a cultural dimension that directly influences the relationship between instructor and student. Research based on the Hofstede cultural model (Hofstede, 1984, pp. 72-78), reveals that countries with low trust in governments, such as parts of Eastern Asia, students tend to be less likely to ask questions or provide objective feedback. On the other hand, in Western cultures, where the approach is more participative, the instructor is often seen as a partner in the learning process, and, most importantly, communication is bidirectional. Thus, the instructor needs to be flexible and adaptable to each situation, recognize these cultural differences and change their teaching style to maintain the desired efficiency in training.

In addition, new technologies and innovative methods used in pilot training, are reshaping the role of the instructor. Modern programs, such as Evidence-Based Training – EBT (Hwang, Kim, 2023, pp. 88-95) and Line-Oriented Flight Training – LOFT (Dismukes et al., 1997, pp. 3-7), encourage instructors to act as facilitators and evaluators of complex performance, focusing on developing adaptive thinking and preparing students for atypical, critical scenarios. According to EASA (2020, pp. 216-218), instructors involved in EBT must be capable to create dynamic situations, evaluate students' skills in a holistic framework and provide detailed feedback aimed at identifying the fundamental causes for errors.

On the same idea, there is a growing awareness of the importance of developing coaching and counseling skills, as an extension of traditional teaching methods. FAA (2020, Ch.7, pp. 4-8) recommends that instructors adopt *learner-centered teaching*, by including constructive feedback, self-reflection and in-depth post-flight debriefing. These practices are necessary to help students develop the abilities to understand and correct their own errors. Research has shown that such an approach benefits not only the technical performance, but also student's self-trust and motivation (Seung et al., 2024, pp. 237-239).

Next, we will go through various roles that an instructor pilot must fulfill in order to meet the current requirements for preparing the best student pilots in the field of aviation.

FLIGHT INSTRUCTOR'S ROLES

The roles of the instructor pilot have evolved significantly over the last two decades, as aviation requirements have become more rigorous. The evolution of international safety standards, the increasing complexity of flight operations, and the integration of non-technical competencies have determined the aviation academies worldwide, such as CAE Global Academy, Lufthansa Aviation Training, Oxford Aviation Academy or Emirates Aviation University to adopt a multidimensional approach to pilot training (Salas et al., 2012, pp. 76-86).

The traditional model centered on the unidirectional relationship between instructor and student has extended to the point where the instructor becomes at the same time a facilitator for learning, coaching, behavior evaluator or mentor. Beyond the ability to pass flying techniques to others, the focus has grown more and more on the development of the non-technical skills, such as communications, decision-making process, stress management, team work and safety culture, essential elements for reducing human errors and enhancing crew performance (Flin, O'Connor, 2008, pp. 27-45).

Mentor

Nowadays, mentorship is recognized as one of the most influential learning methods in high responsibility scenarios, and aviation is a great domain in this sense. The flight instructor acts more and more as a mentor - a quality that drives him to guide students not only in the operational procedures learning process, but also in the development of their professional identity, a healthy attitude towards risk management, responsibility and decision-making process. This role is complex, as it implies cognitive, emotional and social elements altogether, its efficiency being well documented in aviation studies and in organizational literature.

In pilot training, mentorship surpasses the traditional instructor role, becoming an essential mechanism for professional and personal growth for pilots. The instructor-mentor provides not only technical guidance, but also support in shaping values, attitudes and psychological resilience. According to FAA (2020), mentorship contributes to the development of a trustworthy learning climate, in which students feel encouraged to ask questions, make mistakes and reflect on their actions. Based on Kram's model (Kram, 1985, pp. 32-38), mentorship can be divided into two dimensions: instrumental support (guidance, feedback, career planning) and psychological support (emotional encouragement, behavior modeling).

Researchers like Clutterbuck (Clutterbuck, 2004, pp. 47-53) and Goleman (Goleman, 1998, pp. 92-97) emphasize that effective mentors exhibit not only technical expertise, but also empathy, emotional intelligence and reflective abilities, enabling them to build a peer-to-peer relationship with student. Additionally, reflective debrief sessions (Brookfield, 1995, pp. 66-72) contribute substantially to the learning process, stimulating critical thinking and awareness of decision-making process during flight.

Also, many studies conducted by different researchers (Helmreich, Merritt, 2001, pp. 85-90; Reason, 1990, pp. 173-178) shows that active mentorship helps reduce flying operational errors and enforces safety culture.

Leader

In the context of pilot training, the flight instructor inevitably fulfills the role of a leader, not only through operational authority but, more importantly through their impact on organizational culture, student behavior and the development of non-technical competencies. The leadership demonstrated by the instructor directly influences students' attitudes towards responsibility, communication, risk management and safety (Kanki et al., 2019, pp. 70-75, 94-102). Recent research emphasizes that efficient leadership in aviation education involves a relational form of authority, based on emotional intelligence, adaptability and positive influence (Goleman et al., 2013, pp. 34-41; Yukl, Gardner, 2019, pp. 268-273). Also, instructors who demonstrate empathy, active listening and the capacity to build trust, abilities which are specific to a servant leadership approach to development, facilitate not only technical learning but also development of pilots who are aware of their role within a crew, capable to act promptly in both collaborative and autonomous ways.

Studies in the aviation domain consistently show that authoritarian leadership, which is still present in some educational environments, may negatively affect crew communication and inhibit student initiative, which may lead to a growth in the risk of errors (Salas et al., 2012, pp. 76-78), (Helmreich, Merritt, 2001, pp. 79-89). On the other hand, transformational leadership, focused on values, vision and personal development, is associated with superior operational performances and a strong safety culture (Bass & Riggio, 2006, pp. 42-48). This approach is increasingly applied in aviation academies worldwide, where instructors are prepared to be involved in adaptive leadership, team communication and human factors dynamics. Additionally, instructors' leadership skills becomes essential in moments

of uncertainty when stress and error might occur. The FAA Instructor's Handbook (2020, Ch.7, pp. 6-8) highlights that the way an instructor reacts to a mistake or a critical situation, determines the student's attitude towards risk, accountability and reflexive learning in the long term. Thus, adaptive leadership, capable to integrate cultural diversity and cognitive style differences, becomes a strategic component of the modern instructor.

Teacher

The flight instructor, in his role as teacher, does more than simply transmitting knowledge to students. He is responsible for teaching them how to learn and eventually create an applied, reflective and competency-centered approach to learning. Nowadays, the evolution of learning strategies such as CBTA and EBT help instructors to become facilitators of cognitive and operational development, not just followers of a predetermined curriculum (ICAO 2013, pp. I-3-1 - I-3-3; Biggs, Tang, 2011, pp. 97-102).

The teaching process in aviation involves critical thinking stimulation and understanding of flight principles. According to Merrill (2020, pp. 9-13) effective learning must address questions such as *"what?"*, *"how?"* and, most importantly, *"why?"*, in order to help students apply knowledge in complex scenarios. The teacher should adapt instructional strategies to each learner's profile, including cognitive style and experience level, ensuring coherence between learning objectives and specific activities to reach those objectives. Also, the instructor needs to adapt and develop pedagogical skills, which according to Salas et al. (2012, pp. 84-86), are closely correlated with student's performance and evolution. The teacher's role is to find that sensitive link between curriculum objectives and the learning activities and assessments that students need to use to shape their professional judgement for developing the safety culture through every lesson.

Moral evaluator

This role focuses more on cultivating a strong ethical framework that guides students in the decision-making process. The instructor must serve as a model of professional integrity, directly influencing how students perceive and apply safety standards, regulations, as well as their sense of responsibility regarding both crew and passengers (ICAO 2018, Ch.2, pp. 10-14). Besides technical and non-technical knowledge delivered to students; moral evaluation refers to the instructor's ability to identify and correct risky behaviors or attitudes that could undermine safety culture. Even though students manifest a satisfactory technical performance, their behaviors must reflect the safety culture standards.

According to Flin and O'Connor (Flin, O'Connor 2008, pp. 31-45), non-technical skills such as stress management, open communication and ethical decision-making, are required to prevent negative situations in aviation operations. CBTA and EBT frameworks contain ethical attitudes as integral elements, giving instructors the opportunity to provide clear feedback when students show a tendency to compromise safety to the detriment of operational efficiency. This process should lead to the development of moral situational awareness, ability to recognize not only what is operationally possible, but most importantly what is ethically correct.

Coach

Another important role of the instructor is to be a coach for the student. This role represents the motivational dimension through which the instructor supports both learner's professional and personal growth, mostly through guidance towards self-learning process. Coaching emphasizes dialogue, clear objectives, and concise feedback, aiming to shape the learner from a passive performer into an autonomous professional, aware of their own resources (Whitmore, 2017, pp. 9-22). This approach strengthens critical thinking in complex situations, making it easier for the students to go through decision-making process. Studies show that when instructors apply coaching principles, such as guided discovery (finding solutions by going through a scenario by themselves) or post-flight guided reflection, learners improve their ability to correct errors in a timely manner and make better decisions in the future (Salas et al., 2012, pp. 92-95; ICAO 2013, Ch.2, pp. 2-4).

For example, Emirates Flight Training Academy or CAE (Computer-Aided Engineering) are institutions where flight instructors use personalized scenarios for each individual in order to challenge students to find solutions, minimizing direct intervention. This method stimulates personal responsibility and improves self-confidence. Such adaptability to each individual's psychological and cultural profile, complements the role of teacher and leader, adding the dimension of developing professional autonomy and resilience.

Psychologist

In pilot training, the role of psychologist is automatically implied. Besides technical and soft skills, the instructor has to pay attention to the student's mental, emotional and behavioral states. Given the high cognitive and operational stress demand, specific to aviation, the management of these factors needs to be approached as early as the training phase (Salas et al., 2013, pp. 34-40). The instructor-psychologist must be able to identify stress level, anxiety, fatigue or cognitive workload in order

to adjust the pace and complexity of instruction. According to Helmreich and Merritt (2001, pp. 120-124), early recognition of these factors can prevent critical errors and drops in performance. Moreover, the instructor has a responsibility to cultivate psychological resilience, enabling trainees to return quickly to an optimal level of functioning after stressful events (Robertson et al., 2015, pp. 534-536).

This role also requires empathic communication and active listening skills, elements that reduce psychological barriers and encourage students to be open whenever they encounter difficulties (Goleman et al., 2013, pp. 58-77). Emotional expression and stress perception become essential for the success of the training process. While the instructor-psychologist does not replace a clinic specialist, they apply necessary performance and organizational psychology principles in order to observe, interpret and manage critical human factors during flight operations. This role complements both technical and non-technical skills, supporting the emotional and mental balance for a smooth progression of the entire instructional process.

Innovator

One of the most important roles that the instructor has in the flight training is that of innovator, as it reflects the ability to continuously adapt and integrate new technologies, pedagogical methods, and training strategies in response to lessons learned from the past and also the industry's rapid changes. If the leader inspires, the mentor fosters values, and the teacher imparts knowledge, the innovator is the one that uses the necessary tools and approaches to transform the learning process. When we think about innovation, we mostly refer to technology, but the instructor-innovator goes beyond that, by rethinking how training and assessment are designed, adopting active methods such as problem-based learning or adaptive learning (Bellotti et al., 2013, pp. 2-4).

Although technology is not the main pillar, it does support the learning process. The instructor continuously tests hybrid training methods by combining state-of-the-art simulators with collaborative online scenarios to enhance learning efficiency and knowledge retention. In this context, the instructor-innovator plays a double role: first, influencing the student performance, and second, adapting and redefining organizational standards.

When put together, innovation supports leadership by providing up-to-date decision-making tools, enhances mentorship through interactive resources, helps teaching with dynamic modern methods and assists the psychologist role by enabling technologies that can monitor emotional factors in real time.

Risk manager

Lastly, the risk manager is the one role that anticipates, evaluates and controls the variables that might affect safety and performance. By applying the principles of Safety Management System and Threat and Error Management, recognized by ICAO and EASA, as fundamental to diminishing operational risks (ICAO, 2018, pp. 7-14, Ch.2), the instructor must encourage students to continuously be aware of potential risks, contributing to a strong safety culture.

For this reason, after depicting the basic maneuvers of the aircraft, the instructor focuses on engaging students to solve emergency scenarios from simple to more complex situations. Their role is to guide the trainees to rapidly recognize warning signals, make informed decisions, and implement specific measures in real time (FAA, Aviation’s Instructor Handbook - FAA-H-8083-9B 2020, pp. 8-12). The risk manager role is applied throughout all phases of training, from pre-flight briefings (identifying potential risks) to post-simulation debriefings (discussing what could have happened), as well as through the use of adapted checklists, hazard analyses and open discussions regarding errors. The risk manager role is not isolated, but functions as a protective layer that reinforces and optimizes effectively all other functions of the flight instructor.

After understanding the eight roles an instructor pilot must fulfill, it becomes clear that each role has its own contribution to future pilots’ professional and personal development. Even though their purposes are different, the roles are interdependent and complement to each other, creating a complex yet adaptable educational framework. In order to synthesize and highlight both specific and common elements, the following table presents the key dimensions of each role (Table 1).

Table 1: Roles of instructor

Role	Primary Objective	Essential functions	Applicable Methods	Key-moments in training	Necessary competencies
Mentor	Shaping professional values and attitudes	Personalized guidance, behavior shaping	One-on-one discussions, professional storytelling	Early training phases and later when needed	Empathy, practical experience, communication

Role	Primary Objective	Essential functions	Applicable Methods	Key-moments in training	Necessary competencies
Leader	Inspiring towards safety and performance	Clear vision, resource management	Transformative leadership, LOFT	Complex situations, emergencies, team work	Emotional intelligence, decision-making abilities
Teacher	Knowledge sharing	Structured teaching, adapting content	Theoretical lessons, simulation, practical demonstrations	All phases of training	Pedagogy, clarity, feedback
Moral Evaluator	Maintaining ethical standards	Behavior evaluation, correcting deviations	Ethical conversations, feedback	Moral situation through all training	Integrity, impartiality
Coach	Autonomy development, individual performance growth	Motivation, goals setting	Guided reflection, progress planning	Towards the end of training	Active listening, positive communication
Psychologist	Maintaining emotional and cognitive balance	Identifying stress, emotional support	Psychological evaluation	High intensity scenarios, repeated failures	Empathy, emotional intelligence
Innovator	Introducing new methods	Adaptability to changes, testing and implementing innovative solutions	Simulators, adaptive learning	All phases of training, periodic updates	Creativity, adaptability, technological competencies
Risk Manager	Anticipating, mitigating risks	Hazard analysis, error correction	Emergency simulations	Any phase where risk can appear	Critical analysis, under pressure decision-making

INSTRUCTOR PROFILE

From the analysis of the eight roles of the flight instructor: mentor, leader, teacher, moral evaluator, coach, psychologist, innovator and risk manager; we are able to outline a complex and multidimensional instructor profile, which goes beyond the traditional scope of technical training. Each role contributes to drawing the broader picture of pilot development, starting from the technical and operational skills to non-technical competencies, and cumulating in the consolidation of safety culture, flying performance, resilience and professional ethics. For the instructor, this role diversity offers major benefits, allowing them to adapt and refine teaching methods, address the individual needs of students and further to grow their own professional expertise.

The ideal flight instructor, in our opinion, is a professional who exceeds the boundaries of technical training, by combining mastery of flying skills with the capacity to instill values, shape professional ethics and be able to develop resilience, decision-making under pressure and clear communication. Given that pilot training is divided in multiple training phases due to the complexity of flying programs, these roles can be distributed accordingly, depending on the necessities. Therefore, it can be identified a natural distribution across four proposed instructional levels (Figure 1):

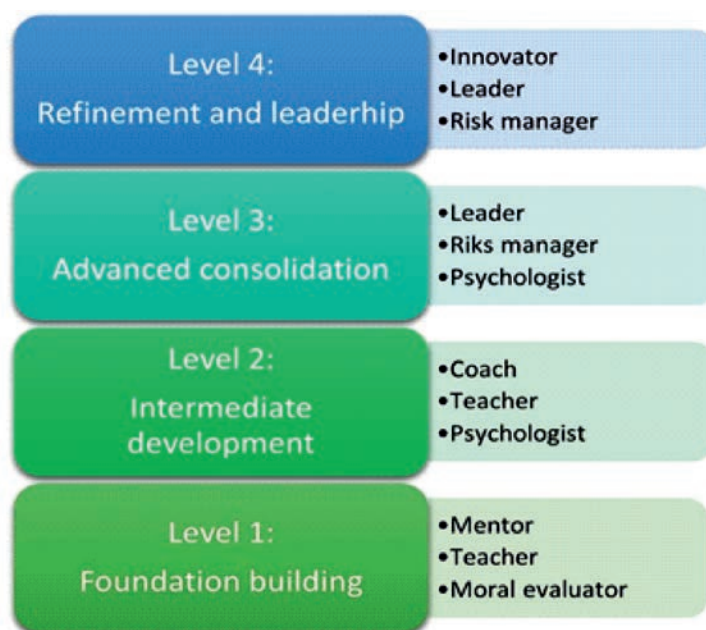


Figure 1: The roles distributed on training phases levels

1. **Foundation building:** This level corresponds to the initial stage of pilot training, where the focus is on building a solid foundation of theoretical knowledge, basic practical skills and safe attitudes. The dominant roles for this stage are the **mentor, teacher** and **moral evaluator**. While the mentor helps creating a trust-based relationship and supports the students' adaptation to aviation environment, the teacher ensures a clear and updated transmission of fundamental principles. The moral evaluator works on ethical standards and safety culture in early interactions with the trainees. This level allows a smooth transition to aviation and gives students the opportunity to adapt as easy as possible. Also, the mistakes are corrected immediately whilst the feedback is more informative than applied, creating strong pillars for the remainder of the training process.
2. **Intermediate development:** At this level, the student is already familiarized with the environment, possesses basic knowledge and begins to develop operational autonomy. Central roles of the instructor are those of **coach, teacher** and **psychologist**. The first one guides the student towards self-assessment and continuous improvement, the second one introduces more complex scenarios and situations where the critical thinking gets involved, and the last one manages the stress and pressure associated with more challenging operations. Unlike the first stage, where interaction was preponderantly one-way, the second level allows for more collaboration, stimulating student's capacity to make clear, independent decisions.
3. **Advanced consolidation:** The student is more comfortable with the environment at this level and is ready to test their limits and ability to respond to increasingly complex scenarios. The main roles that apply to this phase are those of **leader, risk manager** and **psychologist**. The leader creates specific contexts and puts students in situations that require a prompt decision-making process and effective team coordination, the risk manager introduces procedures and advanced techniques to prevent incidents, and the psychologist focuses more and more on maintaining a high performance as the stress levels increase. This stage goes beyond basic elements and involves the full integration of technical and non-technical skills, giving the student the confidence and competences for complex real situations.
4. **Refinement and leadership:** The highest level marks the transition from trainee to professional status, capable of managing aircraft performance, coordinating with the crew, and most importantly, sustaining personal

performance. The key roles in this case for the instructor are those of **innovator, leader** and **risk manager**. The innovator uses new technologies and methods to optimize and adapt performance to the latest standards, the risk manager goes a step higher into refining the pilot's capacity to anticipate, analyze and manage safety threats, whilst the leader manages to cultivate a strong safety culture and a vision oriented to excellence. This stage of training transforms the pilot into a professional ready to be proactive in creating and maintaining a safe and efficient flying environment.

This four-level distributed structure ensures that by the end of the training process, the student is not only technically proficient but also strategically minded, ethically grounded and capable of thriving the multiple challenges that modern aviation encounters.

CONCLUSIONS

This article brings a conceptual contribution to the aviation literature regarding pilot training, by presenting an integrated approach of the instructor pilot roles in correlation with the developmental phases of trainee, the student pilots. Beyond the descriptive analysis of the eight identified roles: leader, mentor, teacher, moral evaluator, coach, psychologist, risk manager and innovator, the article proposes a four-stage logical structure that encompasses the path the instructor must follow in order to support the student pilots to progress in their educational journey. This perspective redefines pilot training, transitioning from a traditional, one-dimensional view of the instructor (as a mere technical expert or procedural trainer) toward a holistic, well-structured, and contextualized vision that integrates both theoretical and practical training. It is very important to understand that the eight roles presented in the article are present in all stages of the training, except that, and it was specified in the text above, for some levels only a few roles are dominant. Rigorous training could only be achieved if these 8 roles are fully present at every moment. The way in which they are applied depends very much on the skill of the flight instructor.

First, in the existing literature, the flight instructor's role is often reduced to a set of pedagogical and technical responsibilities, without a clear structure regarding the professional progress of the student. This study fulfills this gap by integrating professional education theories (Biggs, Tang, 2011; Brookfield, 1995), educational leadership (Clutterbuck, 2004; Goleman, 1998), and operational risk management (Reason, 1990; ICAO 2013) into a coherent framework for phased application.

This framework allows instructors to differentiate where they need to intervene or not, based on task complexity, decision-making level and the student's degree of autonomy.

Second, the article highlights the need of an equilibrium between the cognitive and emotional elements necessary in aviation training. Incorporating the roles of mentor, psychologist and moral evaluator roles alongside operational and technical ones reflects an understanding of aviation as a domain where safety is dependent on technical skills, but more importantly on human interaction quality and decision-making process. Pilot training must include the development of self-reflective capacity, stress management, leadership and adaptive learning, elements that must align with the progressive involvement of the instructor.

This article, also, creates a new research direction on the relationship between roles of instructor and student performance across diverse cultural contexts. As multicultural aspects gain more attention, the four-staged model, proposed in this article, allows flexibility to adjust methods and approaches according to students' cultural expectations, promoting an inclusive and flexible perspective.

Another possible future direction of research is that of studying the impact in terms of the progress of the initial development of piloting skills in military students at the *"Henri Coandă"* Air Force Academy, the higher military education institution responsible for training, among others, military pilots serving the national defense system. The flight training internships, carried out annually during the four years of schooling, are essential stages for shaping them into exceptional pilots, and the way in which the roles played by the instructor are reflected within the specific levels of the training stages is certainly essential in achieving this goal. The modern aircraft currently in the Romanian Air Force, but also the hope of being equipped with state-of-the-art ones, make us look with confidence and hope that what we have presented in this article will constitute that essential element that will help in a much easier transition from school/training aircraft to modern combat aircraft.

In conclusion, modern pilot training requires multiple and adaptive approaches that can help students meet the current standards of aviation regulations and also to enforce a more rigid safety culture. By aligning the eight identified roles with the four progressive levels of instruction, this article bridges technical mastery with non-technical competencies, ensuring that trainees develop not only operational proficiency, but also resilience, ethical judgment and emotional awareness. Ultimately, it positions the flight instructor as a strong element in preparing the most competent, confident and safety-oriented pilots and also updating the organizational environment to the most recent standards.

BIBLIOGRAPHY:

1. Bass, B., Riggio, R. (2006). *Transformational Leadership*. Psychology Press.
2. Bellotti, F., Kapralos, B., Lee, K., Ger, P. M., Berta, R. (2013). *Assessment in and of Serious Games: An Overview*. Advances in Human-Computer Interaction.
3. Biggs, J., Tang, C. (2011). *Teaching for Quality Learning at University*. McGraw-Hill Education.
4. Brookfield, S. (1995). *Becoming a Critically Reflective Teacher*. San Francisco: Jossey-Bass Inc.
5. Clutterbuck, D. (2004). *Everyone Needs a Mentor: Fostering Talent in Your Organisation*. CIPD Publishing.
6. Dismukes, K., Jobe, K, McDonnell, L. (1997). *LOFT Debriefings: An Analysis of Instructor Techniques and Crew Participation*.
7. EASA (2020). *Easy Access Rules for Flight Crew Licencing*.
8. FAA (2020). *Aviation's Instructor Handbook – FAA-H-8083-9B*. Federal Aviation Administration.
9. Flin, R., O'Connor, P. (2008). *Safety at the Shar End, A Guide to Non-Technical Skills*. London: CRC Press.
10. Goleman, D. (1998). *Working with Emotional Intelligence*. Bantam Books.
11. Goleman, D., Boyatzis, R., McKee, A. (2013). *Primal Leadership: Unleashing the Power of Emotional Intelligence*. Harvard Business Press.
12. Helmreich, R., Merritt, A. (2001). *Culture at Work in Aviation and Medicine*. London: Routledge.
13. Hofstede, Geert. (1984). *Culture's Consequences*. Sage.
14. Hwang, E., Kim, J.. (2023). *Success factors of evidence-based training for pilots*. Information Development.
15. ICAO (2018). *Doc 9859-CAO Safety Management Manual*. ICAO – International Civil Aviation Organization.
16. Kanki, B., Jose A., Chidester, T. (2019). *Crew Resource Management*. Academic Press.
17. Kram, K.E. (1985). *Mentoring at Work: Developmental Relationship in Organisational Life*. Academy of Management Journal.
18. *Manual of Evidence-based Training* (2013). Secretary General.
19. Merrill, D. (2020). *First Principles of Instruction*. AECT.
20. Reason, J. (1990). *Human Error*. Cambridge University Press.
21. Robertson, I., Cooper, C., Sarkar, M., Curran, T. (2015). *Resilience training in the workplace from 2003 to 2014: A systematic review*, in *Journal of Occupational and Organizational Psychology*.
22. Salas, E., Driskell, J., Hughes, S. (2013). *Introduction: The study of stress and human performance*. In *Stress and human performance*, Psychology Press.
23. Salas, E., Tannenbaum, S., Kraiger, K., Smith-Jentsch, K. (2012). *The Science of Training and Development in Organizations: What Matters in Practice*. Psychological Science.

24. Seung, J.J., Yoo Jae, H., Wontae, P. (2024). *The Impact of Pilots' Learning Satisfaction and Aptitude on Tension and Confidence*, in *International Journal of Information*.
25. Whitmore, J.. (2017). *Coaching for Performance*. John Murrat Press.
26. Yukl, G., Gardner, W. (2019). *Leadership in Organizations*. Pearson.

OPTIMIZING AN INTEGRATED MAINTENANCE SYSTEM FOR VEHICLES

Colonel Ioan MUNTEANU

Colonel Florin Ioan CIOANĂ

4th "Gemina" Infantry Division, Cluj-Napoca

DOI: 10.55535/RMT.2025.3.39

Configuring military structures, regardless of their specialization, to act in military operations requires a "projection" adaptable to the modern combat environment, as well as to the challenges posed by adapting new technologies to the military environment and even the use of artificial intelligence. Flexibility in approaching calculation methods, mathematical modeling and optimization of the projections of maintenance structures and microstructures will lead to obtaining optimal configurations both as military structures and especially as specific activities.

These can be calculated, modeled and optimized so that their configuration responds to both the missions and objectives as well as the principles of employing military forces in military operations.

Keywords: maintenance; system; design; configuration; optimization;

INTRODUCTION

One of the essential factors in achieving success in a military action or operation is the existence and capacity of a logistics system to ensure the needs of military forces, both those in contact and those in other situations. Regarding the logistical assurance of the military forces in contact, an important element is the existence, capacity and adaptability of the maintenance system of the military equipment used so that the military forces always have a high technical condition coefficient or high level of readiness and that allows them to fulfill the missions received.

The combat power of a military force derives primarily from its combat potential. The combat potential of a force, according to specialized military literature (Buța, Alexandrescu, Dumitru, 2004, p. 10), contains at least two components: the designed combat potential and the available combat potential.

Projected combat potential (du Bois, Hughes jr., Low, 1998, p. 78) refers to the latent capability of a force to achieve useful results in combat, organized, trained, equipped, supported, motivated, and led appropriately for the designated force against a planned threat. Basically, it is that state of physical existence of a military structure resulting from the way of organization, equipping with military equipment and systems, training and preparation for combat and used according to the principles and tactics established by military doctrine.

In the projected combat potential, the logistics support component that includes the maintenance system of military equipment, through its optimal design and configuration, can maximize or minimize the projected combat potential of the military structure.

Available combat potential (Ib.) is the latent ability of a force to achieve optimal results in combat through the existence of organization, training, equipment, support, *including logistical support*, motivation and leadership. The available combat potential of a tactical-level structure represents that initial state of the military structure, influenced by *factors and variables* from the battlespace, and once used in combat can produce planned/expected effects against an enemy.

In order to carry out an analysis, from a mathematical point of view, of the design and configuration of a flexible and adaptable maintenance system that has an available potential necessary for the repair of military vehicles, we will introduce

and *integrate factors, variables and constants* that influence the dynamics of the vehicle maintenance system.

The projection, configuration and optimization of an integrated vehicle maintenance system starts from the fulfillment, at least at the theoretical level, of a **minimum system balance condition**, namely: *the number of operational vehicles at a given moment must be equal to the difference between the number of vehicles with which the military operation begins and the difference between the numbers of destroyed vehicles removed from combat/action and repaired vehicles.* This minimum equilibrium condition, analyzed, broken down into variables and constants and subsequently their optimization, will provide us with the necessary information to configure an integrated vehicle maintenance system. The integration of these variables and constants will be done in accordance with the principles of the use of forces in military operations.

Mathematically, the expression that can ensure the balance equilibrium of the maintenance system can be formulated as follows:

$$N(t+1) = N(t) - (R_l - R_r)$$

where,

- **N(t)** - Number of operational vehicles at the start of combat t (first day of combat)
- **N(t+1)** - Number of operational vehicles after first day of combat;
- **R_l** - Rate of vehicles taken out of battle;
- **R_r** - Rate of repairable vehicles.

For the analysis and development of the mathematical expression that defines the equilibrium condition of the integrated vehicle maintenance system, we establish essential factors, variables and constants, as follows:

- **I(t)**: The number of damaged, immobilized, but repairable vehicles at time t. This number depends on the maximum capacity of the system to repair vehicles in a day;
- **C**: The maximum capacity of the maintenance system to repair vehicles per day.
- **r**: Daily vehicle loss coefficient. It is assigned based on historical data or even by military planners depending on the intensity of military actions/operations. ($0.01 < r < 0.9$);
- **P**: The irrecoverable/irreparable loss coefficient, is the number of damaged vehicles that are irreparably destroyed. $0 < P < 1$. (we assign it according to the type of military action, 0.3 for defense and 0.9 for offensive as an example).
- **R_l** - Rate of vehicles taken out of battle

The rate at which vehicles are damaged or destroyed in a day depends on the total number of operational vehicles at the beginning of that day. The more vehicles there are in the battle, the higher the probability of suffering losses.

Mathematically, the expression is:

$$R_l = r \cdot N(t),$$

where:

- R_l - is the number of vehicles taken out of battle in one day;
- r - is a daily loss coefficient (eg: 0.01-0.15, i.e. 1-15% of the defense fleet);
- $N(t)$ - is the number of operational vehicles at the start of the day/military action.
- R_i - Rate of irreparable losses

Due to the military actions in the battle space from the total number of vehicles taken out of battle R_l , a part P is irretrievably destroyed.

$$R_i = P \cdot R_l = P \cdot r \cdot N(t)$$

- R_r - Rate of repairable vehicles

This is where the ability of the vehicle maintenance system to repair vehicles based on its organization, equipment and optimal operation comes into play. The number of vehicles that can be repaired is the difference between those taken out of battle and those irreparably destroyed, respectively $(1-P)$. Entering the data into a mathematical expression the result is:

$$R_r = R_l - R_i$$

Substituting the terms, we get:

$$R_r = r \cdot N(t) - P \cdot r \cdot N(t)$$

To simplify the calculations, we initially consider only one type of damage.

R_{rep} - Repair rate of the integrated maintenance system vehicles - SMIA

This is the constant capacity of our system, C . The actual repair capacity at any given time is limited by either the maximum repair capacity of the SMIA or the number of damaged vehicles available for repair.

$$R_{rep} = \min(C, I(t)),$$

where $I(t)$ is the difference between retired and repairable vehicles and the repairability of the integrated vehicle maintenance system. Starting from the moment $t+1$, the number of vehicles that remain unrepaired from the previous day is added to the number of damaged/immobilized vehicles $I(t)$. They cannot be repaired due to the limitation imposed by the system's daily repair capacity. These are repairable, damaged/immobilized vehicles already in the system/on hold.

Basically, it is the damaged/immobilized vehicles that exceed the repair capacity of SMIA and for which an action must be initiated. For the first day of military action $I(t)$ is equal to R_r .

We will use mathematical modeling and optimization to evaluate the importance of each variable, constant and factor that can reflect the equilibrium condition of the integrated vehicle maintenance system.

In general terms, *“the model represents an explicit interpretation of the understanding of a situation or at least an idea about this situation. It can be expressed mathematically, through symbols or words, the essential being the description of the entities and the relationships between them. The model can be descriptive or illustrative, but above all it must be useful.”* (Dulău, Oltean, 2008, p. 9).

Optimization represents *“a set of methods and techniques that determine finding the best solution (optimal solution) for a given problem.”* (Buneci, 2008, p. 7).

MATHEMATICAL RELATION FOR SYSTEM DYNAMICS

After defining the variables and constants regarding the balance of the system we can formulate the mathematical relationship that describes the transformation/modification of the fleet of operational vehicles from one day to the next:

$$N(t+1) = N(t) + R_{rep} - R_i$$

or, extended:

$$N(t+1) = N(t) + \min(C, I(t)) - r \cdot N(t)$$

Substituting some terms, we obtain a form in which we have the variables stated above:

$$N(t+1) = N(t) - R_i + (R_{rep} - R_r)$$

Eliminating the brackets, we have the final mathematical relationship:

$$N(t+1) = N(t) - R_i + R_{rep} - R_r$$

Explained, the mathematical model shows that for the next day of combat the number of operational vehicles of the fleet is equal to the difference between the number of vehicles with which the action or military operation began, from which we subtract the number of irreparably destroyed vehicles and add the number of vehicles that can be repaired from the number of existing repairable vehicles.

And, to keep track of damaged/immobilized vehicles that are repairable, the mathematical expression results:

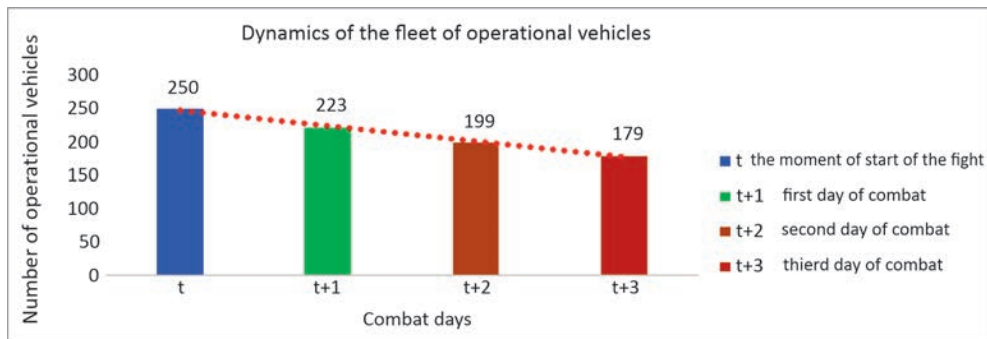
$$I(t+1) = R_i(t) - C + I(t)$$

For the first day of military actions $I(t)$ is equal to R_r , respectively the number of damaged/immobilized and repairable vehicles existing at the end of the day.

Next, we will enter data into the mathematical relationship to observe and analyze the obtained results and calculate, for a tactical level defense operation, for the first three days of combat increasing for each iteration the repair capacity of the integrated vehicle maintenance system by 10 vehicles per day.

The first calculation:

- Total initial fleet $N(t)$: 250 vehicles;
- Daily repair capacity of SMIA, C : 10 vehicle/day;
- Daily vehicle loss ratio r : 15% (0.15);
- The irrecoverable loss coefficient P : 30% (0.30).



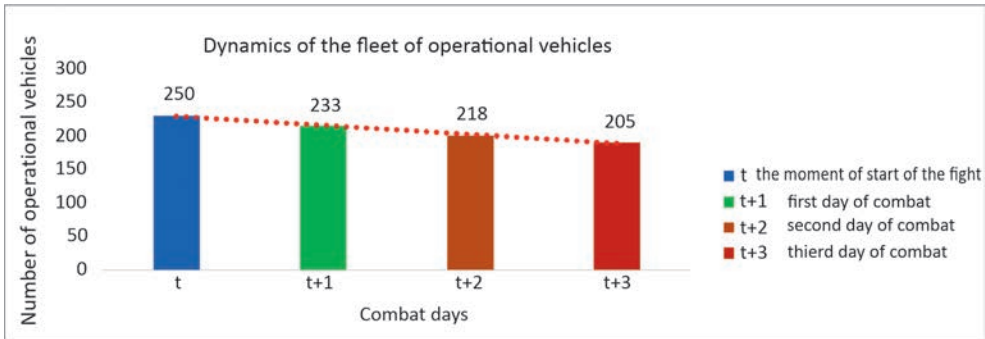
Graph 1: Calculation of fleet dynamics for the first three days of actions with the repair capacity of 10 vehicles per day (author's conception)

The second calculation:

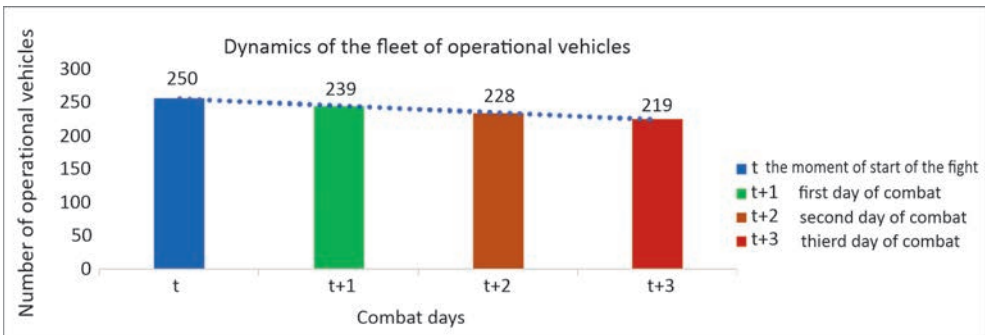
- Total initial fleet $N(t)$: 250 vehicles;
- Daily repair capacity of SMIA, C : 20 vehicle/day;
- Daily vehicle loss ratio r : 15% (0.15);
- The irrecoverable loss coefficient P : 30% (0.30).

The second calculation:

- Total initial fleet $N(t)$: 250 vehicles;
- Daily repair capacity of SMIA, C : 30 vehicle/day;
- Daily vehicle loss ratio r : 15% (0.15);
- The irrecoverable loss coefficient P : 30% (0.30).



Graph 2: Calculation of fleet dynamics for the first three days of actions with the repair capacity of 20 vehicles per day (author's conception)



Graph 3: Calculation of fleet dynamics for the first three days of actions with the repair capacity of 30 vehicles per day (author's conception)

In performing the calculations in the three graphs above we have increased the repair capacity of the integrated vehicle maintenance system from 10 vehicles per day to 30 vehicles per day to analyze how this affects the balance of the system by increasing or decreasing the number of operational vehicles in the fleet. It can be seen that with the increase in the repair capacity, the decrease in the number of vehicles in the fleet is considerably reduced, which results in more operational vehicles and implicitly a higher level of the combat capability of the military structure.

Model evaluation

This mathematical model, even in its empirical form, allows us to make important theoretical estimates, as follows:

❖ If the value of $R_{rep} < R_r$, the number of operational vehicles $N(t)$ will decrease drastically. A "pending repairable vehicle lot" will be created, in which damaged vehicles await repair, they can only be repaired within the limit of the daily repair

capacity, which will lead to a constant and rapid decrease in combat capacity. It can be seen in graph no. 1 that after three days of military actions the number of vehicles in the fleet is 179, a small number for the military structure to achieve the planned results. In this situation, the number of damaged/immobilized vehicles $I(t)$ increases rapidly, which leads to an imbalance of the maintenance system and implicitly on the available potential of the military structure;

❖ If the value $R_{rep} > R_r$, the number of operational vehicles $N(t)$ of the fleet will have an acceptable decrease for the actions of the military structure to be successful. At the same time the number of damaged/immobilized vehicles $I(t)$ will decrease due to the high repair capacity and implicitly all of them will be able to be repaired daily. In this situation the maintenance system is able to cope with the pace of the conflict.

❖ We can ensure the balance of the integrated maintenance system of vehicles by modeling the repair capacity of the maintenance system, respectively increasing or decreasing it. It is useful to maintain the reaction capacity greater than the repair requirement to be able to have an operational reserve of vehicle repairs, just as there are reserves of forces and means for a military action or operation.

❖ Carefully analyzing this mathematical model, it is found that in order to achieve the balance of the integrated vehicle maintenance system, so that at the end of the day the military structure has the same number of operational vehicles or a minimum number that ensures a minimum level of available potential and combat capacity, *it is necessary to introduce a new coefficient* into the mathematical relationship that will represent a stock or a reserve of vehicles to replace irreparably destroyed vehicles.

The SMIA model will be designed/configured and optimized to ensure that, in most scenarios, **the repair capacity/repair rate R_{rep} is greater than or at least equal to the repairable vehicle rate R_r** , thus maintaining an optimal number of operational vehicles necessary to continue military action as planned.

In order to get closer to the reality in the battle space, we will introduce into the mathematical model a **replacement coefficient** of irreparably destroyed vehicles, coefficient hereafter referred to as S , a stock or a reserve located at an optimal distance so that they can be introduced into the battle in a timely manner. Practically, the integrated vehicle maintenance system of the combat forces will be integrated into the logistics lines from the upper echelons. These vehicles can be new or repaired within the maintenance systems of the logistics lines of the upper echelons.

MATHEMATICAL MODEL WITH REPLACEMENT COEFFICIENT

We will keep the irrecoverable loss coefficient **P** defined at the beginning and add the new coefficient **S** for the replacement of damaged/irreparably destroyed vehicles.

We define the terms of the mathematical model:

- **N(t)**: Number of operational vehicles;
- **r**: Daily vehicle loss ratio;
- **P**: The irrecoverable loss coefficient (a portion of damaged vehicles)
- **C**: Daily repair capacity of SMIA.
- **S**: The coefficient of replacement of irreparably damaged/destroyed vehicles (from stock or reserve) representing the ability to reintroduce a number of operational vehicles into battle per day.

Extended mathematic relationship

The dynamics of the operational vehicles number of the fleet from one day to another $N(t+1)$ will be influenced by three factors:

- Irrecoverable losses: Damaged/completely destroyed vehicles, which permanently reduce the fleet;
- Repairs: Vehicles repaired by SMIA and returned to combat;
- Replacements: Operational vehicles will be brought from stock or reserve and used to compensate for losses;

Entering the variables and factors into our model, we will have:

$$N(t+1) = N(t) - (\text{Irrecoverable losses}) + (\text{repaired vehicles}) + (\text{replaced vehicles}).$$

And, in mathematical expression:

$$N(t+1) = N(t) - P \cdot r \cdot N(t) + C + S$$

where,

- **P·r·N(t)** represents the number of vehicles irretrievably destroyed that day;
- **C** represents the vehicles repaired by SMIA and put back into battle;
- **S** represents the number of vehicles in stock or in reserve that replace irretrievably destroyed vehicles.

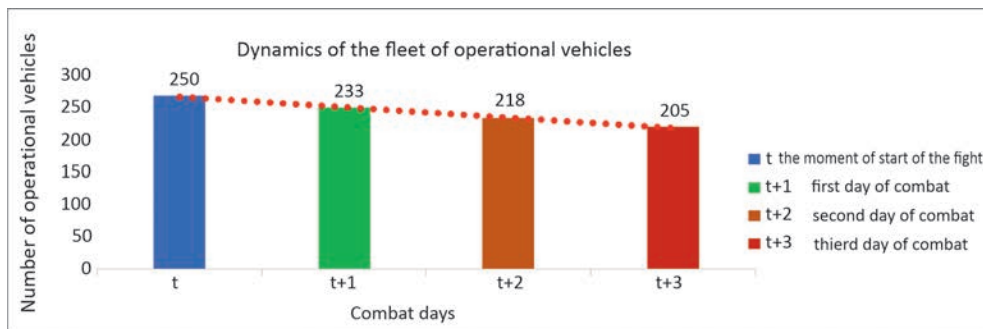
Practical example with replacement coefficient S

Let's say that there are a number of vehicles available in a stock or reserve fully repaired and tested at the level of the higher lines or in nearby, and a number of 10 vehicles per day can be sent to quickly replace breakdowns. The values of **S** can be assigned as a function of the number of vehicles existing at the time.

We will repeat the calculation, using the same inputs, to which we add the replacement coefficient **S**. We will calculate for three iterations increasing the repair capacity by 10 vehicles for each of them and adding the replacement coefficient **S**.

The first calculation:

- Total initial fleet $N(t)$: 250 vehicles;
- Daily repair capacity of SMIA, **C**: 10 vehicle/day;
- Daily vehicle loss ratio **r**: 15% (0.15);
- The irrecoverable loss coefficient **P**: 30% (0.30).
- The replacement coefficient **S**: 10 vehicles per day.



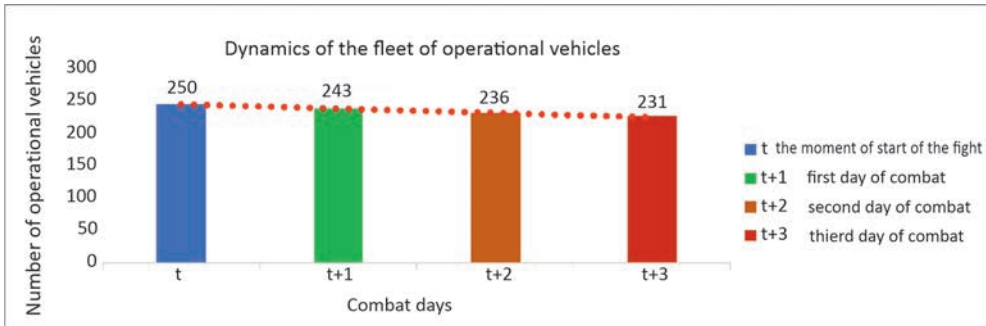
Graph 4: Calculation of fleet dynamics for the first three days of actions with the **S** coefficient and the repair capacity of 10 vehicles per day (author's conception)

The second calculation:

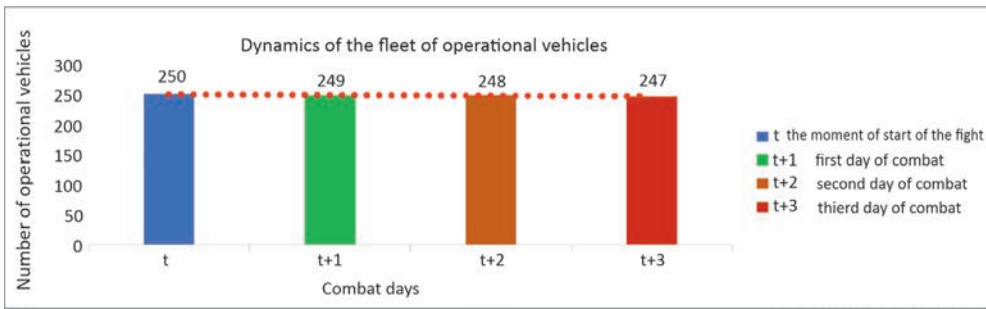
- Total initial fleet $N(t)$: 250 vehicles;
- Daily repair capacity of SMIA, **C**: 20 vehicle/day;
- Daily vehicle loss ratio **r**: 15% (0.15);
- The irrecoverable loss coefficient **P**: 30% (0.30).
- The replacement coefficient **S**: 10 vehicles per day

The third calculation:

- Total initial fleet $N(t)$: 250 vehicles;
- Daily repair capacity of SMIA, **C**: 30 vehicle/day;
- Daily vehicle loss ratio **r**: 15% (0.15);
- The irrecoverable loss coefficient **P**: 30% (0.30);
- The replacement coefficient **S**: 10 vehicles per day.



Graph 5: Calculation of fleet dynamics for the first three days of actions with the coefficient S and the repair capacity of 20 vehicles per day (author's conception)



Graph 6: Calculation of fleet dynamics for the first three days of actions with the coefficient S and the repair capacity of 30 vehicles per day ((author's conception)

EVALUATION OF THE MODEL

In this form the mathematical model shows us that the use of a combined strategy, in which *the repairs carried out by the integrated vehicle maintenance system are supplemented with a stock or a reserve to replace irreparably damaged/destroyed vehicles*, has an amplifying effect on the combat capability of the military structure. In this case, with the daily or periodic replacement, depending on the situation in the battle space, of a stock or reserves of vehicles, the fleet can maintain a certain level of operational capacity, which leads to the maintenance of an available combat power potential.

We can observe that if we set the repair capacity to 10 vehicles per day and replace the irreparably damaged/destroyed vehicles with a stock or reserve, the number of operational vehicles of the fleet can be kept high only for the first two days of combat, i.e. above 85%. By configuring the repair capacity from 20 to 30 vehicles per day and replacing irreparably damaged/destroyed vehicles with 10 per day we can see that the number of operational vehicles in the fleet remains high at 90% for 25 days. Basically, the optimization of the repair capacity

and the replacement ratio will give the optimal configuration of the integrated maintenance system of vehicles.

This optimized form of the mathematical model can give military planners options for designing, configuring, and deploying an integrated vehicle maintenance system to meet the vehicle repair needs of tactical-level military structures in military operations.

This simple exercise demonstrates that under the given conditions, i.e. a repair capacity of 30 vehicles per day and a replacement stock or reserve of 10 vehicles per day, SMIA meets the objective of maintaining a high level of vehicle fleet above 85%.

The model also helps us identify weak points. What happens if the loss rate r increases to 30%? Or if the sunk loss coefficient P increases to 50% due to the lack of rapid evacuation capability? The model allows us to simulate these scenarios and see how we should adjust the repair capacity C and the stock or reserve of vehicles S to compensate for irreparable losses.

MATHEMATICAL MODEL OF OPTIMIZATION

To translate the data into an optimization equation, we need to define an **objective** and the **variables** we can adjust. The key is to find a dynamic balance or resource optimization relationship.

We will use an equation *that balances loss rate with logistics capacity*. We can express it as a balance between the “adverse” part, i.e. the losses, and the “own side part”, i.e. the repair capacity of the SMIA.

Our objective is to keep the operational fleet as close as possible to the initial level, $N(0)$. We can achieve this goal if *the sum of our logistics capabilities equals or exceeds the sum of our losses*.

Textual terms of the equilibrium equation are:

Logistics capacity (own side) $\geq$ Total losses (counterparty).

Repair capacity + replacement capacity $\geq$ repairable vehicles
+ irreparably destroyed vehicles

Translated into mathematically, the equation becomes:

$$C + S \geq R_i + R_r$$

Substituting the terms, we get:

$$C + S \geq r \cdot N(t) + P \cdot r \cdot N(t)$$

This equation allows us to model and optimize both sides.

We will analyze each part of the equation to be able to model and optimize it by adjusting its terms.

Left side of the equation - Optimizing the repair capacity of SMIA

Here, we optimize our resources. **The variables** we can control are:

- **C - repair capacity:** We can increase this value by allocating additional technical staff, designing, configuring and equipping mobile workshops and specific necessary equipment;
- **S - replacement capacity:** We can increase this coefficient by creating a stock or a larger reserve of new or repaired vehicles and ready to be sent into battle at the right time.

The Right Side of the Equation - Threat Modeling

Here, we model the threat using estimates from historical data and tactical assessments. Variables are **influenced by the enemy**, but we can estimate and counter them:

- **r - Daily vehicle loss ratio:** it varies according to the type of conflict. We can estimate it for different scenarios (low, medium or high intensity);
- **P - the irrecoverable loss coefficient:** this value depends on the recovery capacity from the field. We can reduce it by increasing the rapid evacuation capacity (Line I), before the damaged technique is completely destroyed;
- **N(t) - Number of operational vehicles:** this is the dependent variable, which we track to see how it evolves over time and optimize it.

Using the above equation, we can find, at least on a theoretical level, answers to the following questions, such as:

- How much additional technical staff, for repair capacity **C**, do we need to keep the fleet stable, if the loss rate is, for example, 25% ($r = 0.25$) and the unrecoverable losses are 50% ($P = 0.5$)?
- How many vehicles in stock or reserve, **S**, do we need to cover a peak in losses if our repair capacity **C** is exceeded?

The system balance equation helps us dynamically to evaluate the integrated vehicle maintenance system and make informed decisions to allocate existing resources where they are most needed and at the right time.

We will continue with the development of the mathematical model by introducing and integrating *a maintenance response factor*, a factor that has a vital role because the speed of decision and intervention has a direct impact on the number of recoverable vehicles and the efficiency of repairs.

We set **M** to represent *the maintenance response factor* in our model. This coefficient will be a value between 0 and 1 and will directly affect the repair capacity. The maintenance response factor is defined by the available potential of the SMIA and refers to that state of organization and configuration of specific maintenance microstructures, the provision of workshops, sections and maintenance

stands, staffed with the minimum necessary technical staff and the existence of a command and control system capable of planning and coordinating the evacuation and repair of vehicles.

Analysis of the role of the reaction coefficient – M

Definition: **M** represents the efficiency with which the SMIA system detects a breakdown, assigns a team and begins the repair or evacuation process.

- **M=1:** Optimal reaction. Teams are dispatched immediately and the reaction time is minimal, the ideal situation. The actual repair capacity of SMIA is close to its technical maximum capacity;
- **M<1:** Weak, delayed reaction. Delays can be caused by understaffing, slow decisions, parts shortages, poor communications or field access difficulties. The actual repair capacity is greatly reduced, even though the system has a large number of mechanics and workshops.

Impact on repairing capacity: A quick reaction increases the chances of recovering damaged vehicles before they are completely destroyed by the enemy. A slow reaction, a small **M**, increases the probability that a recoverable damage will become an unrecoverable loss.

Development of the mathematical formula with the reaction coefficient

We will integrate the new coefficient **M** into the extended model, focusing on how it affects our repair capacity **C**.

$$N(t+1) = N(t) + M \cdot C - r \cdot N(t).$$

Interpretation of the mathematical formula:

- **Repair capacity:** The expression **M·C** shows that the actual repair capacity of the SMIA system is not the maximum capacity **C**, but the maximum capacity multiplied by the reaction factor **M**. Thus, if the system can repair 30 vehicles per day, **C=30**, but has a reaction factor of only 0.5, **M=0.5**, the actual repair capacity is only 15 vehicles per day.
- **Optimization:** This relationship highlights an essential direction: to maximize efficiency, it is not enough to just increase the number of workshops and mechanics in the repair capacity **C**. We also need to invest in command and control systems, communications and rapid decisions to increase the **M**-reaction factor.
- **Maintenance reaction factor **M**** directly affects responsiveness by increasing or decreasing the number of repairs based on the battle conditions in the battlespace. As an example, **M** also reflects the fact that a slow decision delays evacuation movement, the start of work, and, implicitly, reduces the total number of repairs completed in a given period of time, which affects the combat power of the forces.

The mathematical formula with the maintenance reaction factor M and the replacement stock or reserve S

Integrating the maintenance reaction coefficient M to the existing model we will obtain the mathematical formula:

$$N(t+1) = N(t) + M \cdot C - r \cdot N(t) + S$$

The optimization condition:

In order for the operational fleet not to diminish, we need to ensure that the term of growth through repair and replacement is at least equal to the term of loss/removal from combat.

$$M \cdot C + S \geq r \cdot N(t)$$

This equation allows us to ask an essential question: *“What is the minimum value of M that we need to keep the fleet stable taking into consideration our maximum capabilities?”*

We can express this mathematically as a critical equilibrium condition:

$$M_{\text{equilibrium}} = C \cdot r \cdot N(t)$$

If our actual M value is greater than $M_{\text{equilibrium}}$, the fleet increases. If it is less, the fleet decreases.

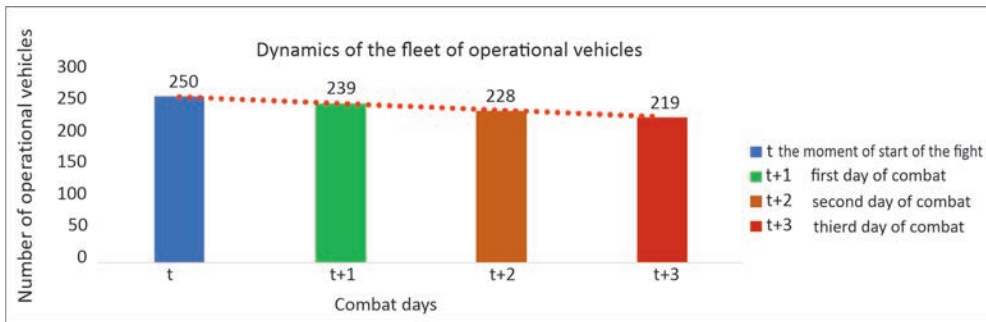
Applying the model to a simulation scenario

Input data:

- Total initial fleet $N(t)$: 250 vehicles;
- Daily repair capacity of SMIA, C : 20 vehicles/day;
- Daily vehicle loss ratio $r = 10\%$ (0.1).
- The irrecoverable loss coefficient P : 30% (0.30);
- The maintenance reaction factor, $M = 0.5$, due to slow communication systems, the existence of a shortage of parts, the insufficiency of means of transport and evacuation, the unavailability of technical personnel at the time, etc.;
- The replacement coefficient S : 5 vehicles per day.

After entering the input data into the mathematical formula we obtain:

- Total daily losses (taken out of battle): $R_l = r \cdot N(t) = 0.1 \cdot 250 = 25$ vehicles taken out of battle;
- Irreparable losses: $R_l P = r \cdot N(t) = 0.3 \cdot 0.1 \cdot 250 = 7,5 \approx 8$ irreparably destroyed vehicles;
- Number of repairable vehicles: $R_l - R_l P = r \cdot N(t) - P \cdot r \cdot N(t) = 17,5 \approx 17$ repairable vehicles;
- Actual repair capacity: $M \cdot C = 0.5 \cdot 20 = 10$ repaired vehicles;
- Operational fleet at the end of day 1: $N(t+1) = 239$ vehicles;
- Operational fleet at the end of day 2: $N(t+2) = 228$ vehicles;
- Operational fleet at the end of day 3: $N(t+3) = 219$ vehicles.

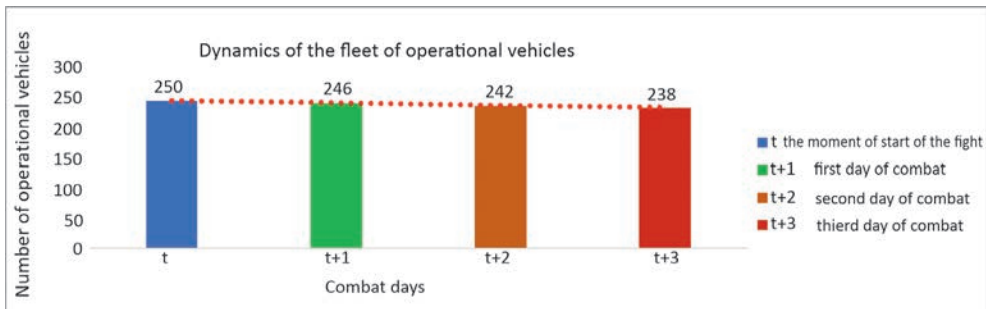


Graph 7: Calculation for the first 3 days with the maintenance reaction factor and replacement stock (author's conception)

Simulation evaluation with maintenance reaction factor and replacement stock

The maintenance reaction factor, after integration into the mathematical model and simulation, reduces the number of operational vehicles in the fleet because the conditions that led to the assignment of the value of 0.5 are real and existing in the battlespace and directly influence the reparability of the SMIA. Analyzing the results for the three days of combat in graph no. 7, we can see that even with the maintenance factor of 0.5, the number of vehicles is above the minimum level of 85%, a minimum level necessary to maintain a high available potential of the military forces and implicitly to continue the missions received.

To observe the impact of the maintenance reaction factor M we will repeat the calculation with the same input data minus its value which we will increase to $M = 0.9$ which means that SMIA has an optimal configuration of workshops, sections, personnel and equipment as well as the functional command and control system with a functional observation, evacuation and repair system that ensures the detection/observation, evacuation and rapid repair of a motor vehicle.



Graph 8: Calculation for the first 3 days with increased maintenance reaction factor and replacement stock (author's conception)

Doing the calculation with the value of $M = 0.9$, for three days of combat, we can observe, in graph no. 8, that the number of operational vehicles is higher than if the value of the maintenance factor M was $M = 0.5$. This demonstrates that the maintenance reaction factor has a major impact on the dynamics of repaired vehicles in a combat day and implicitly on the repair capacity of SMIA.

In order to have a reaction factor M as high as possible and implicitly increase the number of vehicle repairs, peacetime investment in command and control is as important as investment in workshops and specialized technical personnel.

CONCLUSIONS

The success of a military structure planned to carry out military actions or operations is determined, among many others, by the ability of the logistics system to ensure the needs of these forces, including the existence of a vehicle maintenance system. This integrated vehicle maintenance system can be designed and configured by using mathematical modeling and optimization to obtain and use the optimal maintenance structure with the least resources. Also, this maintenance system must be able to integrate and adapt the factors, variables and coefficients that influence its operation, in our case the repair capacity, the stock or reserve of vehicles and the maintenance response factor.

The integration of the factors, variables and coefficients that influence or have an impact on the actions in the battle space in a mathematical model and their optimization generates directions for the design and configuration of an integrated maintenance system of vehicles to meet the equilibrium condition, respectively to be able to ensure the repair needs of the military forces in military operations.

Through the given examples of the use of mathematical modeling and optimization, we observe how the equilibrium condition of the integrated vehicle maintenance system, optimized with the maintenance reaction factor and the replacement coefficient of irreparably destroyed vehicles, helps us to quickly evaluate the performance of the logistics system and especially its component elements that have a direct impact on maintaining the number of operational vehicles of the vehicle fleet. These models, developed and optimized, allow military planners and decision-makers to identify where to allocate additional resources (for example, increasing the repair capacity for certain periods of time of the conduct of military operations, allocating more vehicles as a stock or replacement reserve and at time intervals established by scientific calculations and not by estimates, creating a reserve of maintenance resources, etc.) to keep the available potential and combat power of the forces at a minimum level that ensures their success.

BIBLIOGRAPHY:

1. Col. Bălăceanu, I., col. Dumitru, D., col. (r.) Ioana, I. (2006). *Potențialul de luptă al forțelor terestre în context NATO*. București: Editura Top Form.
2. Buneci, M.R. (2008). *Optimizări*. Târgu-Jiu: Editura Academica Brâncuși.
3. Buța, V., Alexandrescu, G., Dumitru, D. (2004). *Elemente dinamice ale câmpului de luptă modern – Puterea de luptă*. București: Editura Universității Naționale de Apărare.
4. Du Bois, E.L., Hughes Jr., W.P., Low, L.J. (1998). *A Concise Theory of Combat*, The Military Conflict Institute.
5. Dulău, M., Oltean, S. (2008). *Modelare și simulare, Curs*. Târgu Mureș: Universitatea "Petru Maior".
6. FM 100-17-3, *Reception, Staging, Onward Movement, and Integration, distribution restriction: Approved for public release; distribution is unlimited*, Headquarters, 1999.
7. Col. dr. ing. Ghiță, Al. ș.a. (1993). *Analiza cantitativă a datelor istorice despre lupte*, București: Editura Academiei Tehnice Militare.
8. Major Johnson, R.L. (1990). *Lanchester's Square Law in Theory and Practice*, School of Advanced Military Studies. SUA: Fort Leavenworth, Kansas.
9. *Leader's guide to maintenance and services* (2023). Army Center for Lessons Learned. SUA: Fort Leavenworth.
10. Lupșa, L., Blaga, L. (2007). *Special Type of Transportation Problems*, Automation Computers Applied Mathematics, vol. 16, nr. 2.
11. *NATO logistic handbook, Logistic functions* (1997).
12. Nica, V.T. (2011). *Cercetări operaționale I, Introducere în cercetarea operațională, elemente de programare liniară, analiza drumului critic, Introducere în programarea neliniară*. București: Editura ASE.
13. Pawelczyk, M. (2018). *Contemporary challenges in military logistics support*. Polonia: War Studies University.
14. Roman, M. (2012). *Analiza multicriterială. Manual*. București.
15. https://en.wikipedia.org/wiki/Military_logistics, retrieved on 8 August 2025.
16. https://florinleon.byethost24.com/Curs_IA/IA05_Optimizare2.pdf?i=2, retrieved on 10 September 2025.
17. <https://sadat.com.tr/en/kategori/en/turnkey-solutions/products/>, retrieved on 10 September 2025.
18. <https://warfarehistorynetwork.com/article/hein.z-guderian-author-of-the-blitzkrieg/>, retrieved on 20 September 2025.
19. <https://warontherocks.com/2019/02/a-vicious-cycle-the-u-s-militarys-maintenance-and-modernization-problem/>, retrieved on 10 September 2025.
20. https://www.army.mil/article/282460/enabling_rapid_repair_capability_at_echelon, retrieved on 25 September 2025.
21. <https://www.nato.int/docu/logi-en/1997/lo-106.htm>, retrieved on 12 September 2025.

THE ROMANIAN DIPLOMATIC INITIATIVE OF THE “NEUTRAL BLOC” IN THE POLITICAL-MILITARY CONTEXT OF THE BLACK SEA (SEPTEMBER-DECEMBER 1939)

Dr. George-Daniel UNGUREANU

“General Grigore Constandache” Central Archive Depository, Pitești

DOI: 10.55535/RMT.2025.3.40

The dramatic developments between 21 August and 28 September 1939 had a substantial impact on the Black Sea region. The new course of Soviet policy caused deep unease in Bucharest, astonishment in Ankara, and enthusiasm in Sofia. In this context, in September 1939, Romanian diplomacy, led by Grigore Gafencu, pursued several regional objectives, which were summarized at the end of October in the „Neutral Bloc” project. However, the idea of a potential bloc of neutral states in southeastern Europe, under the Italian aegis, had already been discussed and analyzed in various European diplomatic circles since September. This article reviews the preliminary phase of this initiative, the reactions of the European Great Powers and of the small and medium-sized states aimed by Gafencu’s plan, as well as the failure of this ambitious project. Sources list includes Romanian military and diplomatic archives, as well as published Romanian, Turkish, and Soviet diplomatic documents.

Keywords: 1939; Neutral Block; Grigore Gafencu; Italy; USSR;

INTRODUCTION

The dramatic diplomatic, military, and political-territorial developments between 21 August and 28 September 1939 (the creation of the monstrous German-Soviet partnership, the German attack on Poland, and its division between Germany and the USSR, the declarations of war by Great Britain and France against Germany), also disrupted the regional context in the Black Sea area. The outbreak of war between the Great Powers of Western Europe (with the exception of Italy) was perceived in Bucharest as a victory for the USSR, which thus gained great freedom of movement (i.e. expansion) in Eastern and South-Eastern Europe. For Romania, a traditional ally of France and Great Britain, the Soviet Union represented a greater threat than Germany, with which it did not share a border and which could be “*appeased*” through economic concessions (exports of oil, grain, and other raw materials), whereas the Soviet danger was threefold: political, territorial (the issue of Bessarabia), and ideological (Hayness, 2003, pp. 125-126).

Under these circumstances, Romanian diplomacy sought new formulas likely to increase security in South-Eastern Europe, maintain peace and stability in this part of the old continent, and, last but not least, defend the territorial integrity of the Romanian state. Essentially, several major objectives were pursued, namely avoiding entry into the war, consolidating the Balkan Entente, achieving *détente* in the relations with the small revisionist neighbouring states, Bulgaria and Hungary, and developing relations with Italy, the only Western Great Power remaining outside the conflict. In the months leading up to the outbreak of war, Romanian-Italian military relations had been on the rise, particularly in terms of air and naval cooperation (Dobrinescu-Pătroiu-Nicolescu, 1999, pp. 251-255), and Romania’s declaration of neutrality was accompanied by a warm message from Charles II to the leaders in Rome, who were considered guarantors of peace in the Balkans (Ib., p. 243). There were also a significant number of Romanian attempts to contribute to a possible reconciliation between Germany and the Franco-British tandem, in order to limit the Soviets’ room for maneuver. Thus, in the first half of November 1939, King Charles II joined the peace initiative of the sovereigns of Belgium and the Netherlands, making a series of otherwise futile approaches to the three belligerent states (IPERD, 2003, p. 320).

The objectives of Romanian diplomacy in the new regional and continental context were summarized at the end of October in the so-called “*Neutral Bloc*” project, finalized on 28 October 1939, by Foreign Minister Grigore Gafencu, after consultations with the Romanian ambassadors to Türkiye, Greece, and Yugoslavia (Dobrinescu-Pătroiu-Nicolescu, 1999, pp. 245-246). This regional structure was supposed to bring together no fewer than seven states, namely the four member states of the Balkan Entente, plus Hungary, Bulgaria, and a major power, namely Italy. The Romanian diplomatic initiative was probably also boosted by the creation of the Oslo Group by six neutral states in northern and western Europe: Sweden, Norway, Denmark, Belgium, the Netherlands, and Luxembourg (Stănciugel, 2008, p. 201).

The draft, sent two days later to Romania’s diplomatic representatives in Ankara, Athens, Belgrade, Paris, London, Berlin, Rome, Budapest, Moscow, and Sofia, stipulated:

- “*Neutrality in the current conflict*”;
- “*Non-aggression between member states*”;
- “*Adopting a position of benevolent neutrality by the participating states, in case one of them was attacked*”;
- “*Normalization of military measures at common borders*”;
- Contacts between the foreign ministers, and exchanges of political, diplomatic, and military information of mutual interest;
- Economic collaboration between the member states.
- The nature of the bloc was to be entirely defensive, not directed against any third power (IPERD, 2003, p. 320).

This ambitious diplomatic project was to be implemented in two stages, with the governments in Rome, Sofia, and Budapest only being included in the second stage, after a full agreement had been reached between the Balkan allies; until then, only a number of surveys or explorations had been carried out in addition to the three governments (Dobrinescu-Pătroiu-Nicolescu, p. 246). However, as we shall see, the governments initially notified also conducted a series of surveys with third countries, which meant that the details of the Romanian project became known quite quickly in European diplomatic circles.

Virtually, the history of this Romanian diplomatic initiative began on 21-22 September 1939, when the first proposals to take over the leadership of a neutral Balkan bloc were sent from Bucharest to Rome (Marzari, 1970, pp. 771-772), and it was to end on 16 December 1939, when, during a speech delivered before

the Chamber of Fasci and Corporations, the head of Italian diplomacy and Benito Mussolini’s son-in-law, Galeazzo Ciano, dealt the final blow to Romania’s last hopes of co-opting Italy into a neutral regional political project, which had been partially revived after the communiqué of the Grand Fascist Council of 5 December, which referred to maintaining peace in the Balkans, and to Italy’s special interests in this area (Ib., pp. 786-787).

In what follows, we will first review how the five Great Powers of the then Europe related to the Balkans and the Black Sea area in the last third of 1939, then the two major stages in the evolution of Romanian diplomatic efforts to establish a regional bloc of neutral states, with the participation and even under the aegis of Italy, namely the stage prior to, and the stage following the systematization of this project at the end of October 1939.

THE GREAT POWERS AND SOUTH-EAST EUROPE (SEPTEMBER-DECEMBER 1939)

In the months preceding the outbreak of World War II, the Soviet Union was by far the most powerful state bordering the Black Sea, not least in terms of air and naval power, while Türkiye played a key role in the region, both geopolitically (control of the Straits) and politically and diplomatically, as a state with a traditionally privileged relationship with the USSR, and also allied with Romania, Greece and Yugoslavia within the Balkan Entente, as well as in a process of strengthening relations with France and Great Britain. Romania was trying to preserve the unity of the Balkan Entente, given the growing differences between Türkiye and Yugoslavia, while Bulgaria hoped to satisfy some of its territorial claims peacefully, primarily concerning Southern Dobruja (Ungureanu, 2024, pp. 770-773). The news of the conclusion of German-Soviet economic and political arrangements aroused deep unease in Bucharest, astonishment in Ankara, and enthusiasm in Sofia (Ib., pp. 793-795).

Indeed, during his long visit to Moscow between 25 September and 17 October, the head of diplomacy in Ankara, Şükrü Saracoğlu, was confronted with the Soviets’ strident tendency to subordinate Türkiye’s foreign policy to the Kremlin’s new orientations. Basically, the Soviet Union wanted control over the Straits by installing air and naval bases in their vicinity (despite the provisions of the Montreux Convention), but also to cause Türkiye to distance from France, Great Britain, and its Balkan allies, including Romania, which had territorial disputes with both its large eastern neighbour and Bulgaria. The content of the talks, held on 1 October 1939,

between the Turkish foreign minister and I.V. Stalin and V. M. Molotov (DVP, II, 1992, doc. 654, pp. 146-153), is still most significant and telling.

Another worrying signal came from Moscow at the end of October 1939, when, in a speech delivered before the Supreme Soviet, V. M. Molotov declared that the traditional notions of “aggression” and “aggressor” had become obsolete and inadequate for the new stage of concrete evolution of international relations (Dobrinescu-Pătroiu, 1992, p. 16). This statement called into question numerous commitments previously made by the Soviet Union, such as the Conventions on the Definition of Aggression and Aggressor (London, 3-5 July 1933), and appeared as a potential justification for possible and increasingly likely military action against some of the signatory states of the above-mentioned act, including Romania.

The loss of Turkiye’s privileged position in relation to the USSR at the regional level benefited Bulgaria, which, however, in the first decade of October 1939, declined the Soviet offer to conclude a mutual assistance treaty similar to those just signed by Estonia, Latvia, and Lithuania (Ungureanu, ib., p. 796).

Nazi Germany, which had major economic interests in the Balkans related to the supply of raw materials, did not want tensions to escalate, let alone hostilities to spread in this geographical area, but it was also not interested in a profound and lasting improvement in relations between the states of South-Eastern Europe, a development that would have reduced its room for maneuver in relation to them. As historian Frank Marzari observes, London and Paris wanted collective neutrality for the small and medium-sized states of South-Eastern Europe, while Berlin preferred the individual neutrality of those states (Marzari, ib., pp. 769-770). Eloquent in this regard is the message conveyed directly by Joachim von Ribbentrop in early September 1939, during an official visit to Budapest; the head of German diplomacy warned Hungary not to attack Romania under any circumstances, but also not to conclude any non-aggression pact with it (IPERD, 2003, p. 318). Also in September 1939, Germany reiterated the message sent in July to Sofia that the Reich would not look favourably on Bulgaria’s participation in an attack on an economically cooperative Romania (Genchev, 1998, p. 102). During discussions with Galeazzo Ciano on 1 October 1939, Adolf Hitler stated that if Romania did not maintain strict neutrality, Germany would be forced to fully support Russia, Hungary, and Bulgaria in order to “*liquidate the Romanian problem*” (Oprea, 2003, pp. 198-199).

As a matter of general principle, the idea of a neutral bloc of Balkan states had been approved in London as early as mid-September 1939 (Marzari, ib., p. 781).

Even earlier, in the second week of the same month, Ciano and Mussolini had concluded that the formation of a bloc of neutral states in South-Eastern Europe, under Italy’s aegis, could have been beneficial in the long term not only to Italian interests, but also to German interests. The plans to attack Greece and Yugoslavia, finalized in August, were thus canceled (Ibid., pp.770-771).

Hitler was also concerned about the possibility of Italy taking hasty action in the Balkans, which would have created economic difficulties for Germany, so he sought to temper Italian-Soviet tensions, fearing the consequences of possible Italian imprudence more than Soviet expansionism in this part of Europe (Cliadakis, 1974, p. 177).

The conclusion of the German-Soviet agreements in August 1939 had led, almost ipso facto, to the deterioration of Moscow’s relations with London and Paris. However, the two great Western European democracies wanted to maintain communication with the Soviet Union, in the hope of subsequently improving relations with that great power. In their contacts with their Soviet counterparts, British (and French) diplomats sought, without much success, to highlight the danger that German expansion in South-Eastern Europe posed to the USSR (see DVP, II, 1992, passim). For example, on 29 November 1939, on the eve of the outbreak of the “*Winter War*”, Richard Austin Butler, Lord Halifax’s deputy at the Foreign Office, tried to convince the Soviet ambassador in London, Ivan M. Maiski, that Soviet and British interests in the Black Sea and the Balkans were convergent, with both great powers interested in stopping German expansion. In that context, the British diplomat told his Soviet counterpart that “*the fate of Bessarabia is of no concern to England*” (Sturza, editor, 2016, pp. 258-259).

THE UNSYSTEMATIC STAGE OF THE PROJECT

After the shock of the Soviet invasion of eastern Poland (17 September 1939), at the beginning of the last third of the first month of war in Europe, there were also some positive signs for the stability of the South-Eastern part of the continent, with the involvement of Italy. Thus, on 20 September, the joint Italian-Greek declaration was issued, and in the days that followed, a tacit Romanian-Hungarian agreement, mediated by Italian diplomacy, was reached on reducing the military forces massed near the common border (Marzari, ib., pp. 778-779).

Also on 20 September 1939, in Ankara, Ambassador Vasile Stoica had a meeting with Şükrü Saracoğlu, during which the head of Turkish diplomacy indicated that Great Britain and France had given their approval for the Republic of Türkiye

to participate in a regional bloc of neutral states, yet subject to the Turkish state's compliance with the commitments it had made to the two great powers on 12 May and 23 June 1939, respectively. The head of Turkish diplomacy was also optimistic about obtaining the favourable opinion of the Soviet Union (RPMROT, II, 2024, doc. 57, pp. 181-182). The progress and final outcome of the discussions in Moscow with Stalin and Molotov would prove that initial optimism to be unfounded. On 24 October, Saracoğlu would note, in front of the same interlocutor, that the Soviet Union had resumed the expansionist policy of imperial Russia (Cojocaru, 2014, pp. 206-207).

The Romanian diplomatic attempt to negotiate a non-aggression pact with the USSR, based on the territorial status quo, undertaken in the context of the Soviet declaration of 18 September regarding the Soviet state's neutrality towards Romania, also ended in failure (Ungureanu, *ib.*, p. 786). Furthermore, on 20 September V. M. Molotov categorically reproached the Romanian minister in Moscow, Nicolae Dianu, for Romania's hosting military refugees from the disintegrating Polish army (RRS, II, 2003, doc. 123, pp. 252-253). In a less blunt but rather ironic manner, Molotov's assertions were repeated the next day by the Soviet ambassador in Berlin, Aleksandr Shkvarchev, in front of the Romanian diplomat Radu Crutzescu (DVP, II, 1992, doc. 622, p. 120). Quite surprisingly, in the last week of September 1939, some Soviet diplomats gave reassurances to their Romanian colleagues accredited in the capitals of third countries (Lungu, Negreanu-editors, 2000, doc. 24-25, pp. 195-197). At the beginning of October, diplomat Gheorghe Davidescu succeeded Nicolae Dianu as minister plenipotentiary in Moscow, and Romania's new prime minister, Constantin Argetoianu, approved the request of the Soviet chargé d'affaires in Bucharest, Pavel G. Kukoliev, regarding the entry and distribution in Romania of 400 copies of the newspaper *Izvestiya* (RRS, II, 2003, doc. 130, p. 163).

Beyond the contradictory and confusing signals sent by Soviet diplomats, Romanian decision-makers also received information about Moscow's position through other channels. As evidenced by the content of the telegram sent on 9 October by Vasile Stoica, Romanian diplomatic circles were aware of Soviet demands on Türkiye regarding the Straits (RPMROT, II, doc. 63, pp. 186-187).

Soviet intentions to monopolize the Black Sea were also described in the 10 October telegram from the Romanian military attaché in Türkiye, Lieutenant-Colonel Traian Teodorescu (*ib.*, doc. 64, pp. 187-188). Consequently, on 11 October Grigore Gafencu sent Vasile Stoica a telegram with the following content: "*Given*

that in today's times we have a vital interest in not remaining alone in the Black Sea and with the Straits closed, for any circumstance, you will make every effort to ensure that the possibility of assistance is not suppressed.” (ib., doc. 65, pp. 188-189). The head of Romanian diplomacy had in mind the possibility that the British and French military fleets could transit the Straits to come to Romania's aid in the event of an attack on the Romanian state.

Sofia was also aware of Soviet pressure on Türkiye, also on the issue of Ankara's policy in the Balkans, as evidenced by the content of a telegram sent from the Bulgarian capital by Italian diplomat Giorgio Talamo on 10 October 1939, after a discussion with the head of the Bulgarian government and diplomacy, Georgi Kyosseivanov (IID., T2, 1993, part II, doc. 46, p. 363). A few days later, several Bulgarian newspapers reported that the stagnation of the Soviet-Turkish talks in Moscow was allegedly due to the Turkish side's refusal to accept the Soviet point of view on Bessarabia, and to making representations to the Romanian government for a “*peaceful resolution of the Bessarabia issue*” (Fond 71/Türkiye, vol. 61, l. 244).

However, in mid-October, Romanian-Hungarian and Romanian-Bulgarian relations were going through a period of calm, even a relative *détente* (Stănciugel, 2008, p. 201). However, the regional political equation was further complicated by the firm refusal of the Greek leader, General Ioannis Metaxas, to accept the idea of any territorial concessions to Bulgaria, on the part of the member states of the Balkan Entente (Tudorancea, 2011, pp. 158-160).

Also in mid-October, French military sources confirmed the information held by the Romanian General Staff regarding the concentration of Soviet troops in three areas located near the Romanian border, namely north of Cernăuți/Chernivtsi, 140 kilometers west of that city, and along the Tiraspol-Odessa railway line (Constantiniu, 2002, p. 110, note 3). Although he acknowledged that Great Britain and France were unable to provide Romania with prompt and consistent assistance in the event of a Soviet aggression, the British minister in Bucharest, Reginald Hoare, reproached the Romanians for their tendency to see Germany as a counterweight to the Soviet threat (Dobrinescu-Pătroiu, 1992, pp. 14-15).

On 17 October 1939, Şükrü Saracoğlu's long visit to the Soviet Union ended without any noticeable result. On the same day, G. Ciano informed the German ambassador in Rome, von Mackensen, of Italy's decision to abandon its intention to participate in a regional bloc of neutral states (Marzari, ib., p. 774). That decision was not made public until two months later, either because of Mussolini's arrogance,

or because of the internal bureaucratic inertia of the Italian diplomatic apparatus (Ibid.), which fueled the illusory hopes of Romanian diplomacy.

The issue of creating a Balkan (South-East European) bloc of neutral states under Italy's leadership had been discussed during the Hitler-Ciano talks on 1 October, when the Führer agreed only to the idea of a (strictly) Mediterranean bloc, i.e. without the participation of Romania, Bulgaria, and Hungary (Cliadakis, 1974, p. 177). According to L. Marzari, Hitler saw the creation of this potential bloc under Italy's leadership as an opportunity to amplify the Italian-British maritime rivalry, while Ciano aimed to consolidate both Italy's neutrality and Italian influence in South-Eastern Europe (Marzari, 1970, p. 773).

On 18 October Lieutenant Colonel Traian Teodorescu sent a report from the Turkish capital to the Second Intelligence Section of the Romanian General Staff regarding the failure of the Turkish-Soviet negotiations in Moscow. According to the Romanian military attaché, the negative outcome of the discussions was likely due to the Turkish side's rejection of two Soviet demands, namely the inclusion of a "German clause" in the text of the future bilateral mutual assistance treaty (the Soviet Union was not willing to support Türkiye in the event of aggression by Germany), and Türkiye's assuming the obligation to declare war on non-Black-Sea states that would attempt to violate a possible decision to close the Straits (RPMROT, II, doc. 68, pp. 191-192).

On the same day Grigore Gafencu sent a telegram to Vasile Stoica requesting information on the position of decision-makers in the Republic of Türkiye regarding the "*bloc of neutral Balkan states*" (including Bulgaria), but also on the possibilities of cooperation with Hungary and Italy (Ib., doc. 67, pp. 190-191).

The following day, on 19 October 1939, the Anglo-French-Turkish Treaty was concluded, which, according to historian Türkkaya Ataöv, caused "*chagrin in Moscow, wrath in Berlin, and misgivings in Rome*" (Ataöv, 1965, p. 62). Following that act, Germany and Italy vehemently contested Türkiye's status as a neutral state and, implicitly, raised objections to its participation in a potential neutral bloc of states (Ekrem, 1993, p. 106). However, Türkiye had no objections to Italy's possible participation, despite the formal existence of the Berlin-Rome-Tōkyō Axis (Ib., p. 107), which had nevertheless proved ineffective at the time of the conclusion of the German-Soviet agreements.

The act of 19 October 1939 also contained the traditional "*Russian clause*", namely Türkiye's unwillingness to engage in armed conflict with the USSR

and to admit of, or participate in, political-military actions likely to lead to such a conflict (IPERD, 2003, p. 320). This did not prevent the newspaper *Izvestiya* from assessing that Great Britain and France had thus succeeded in drawing Türkiye into the war, attributing the failure of the Turkish-Soviet talks prior to 19 October to Türkiye’s failed attempts, instigated by Great Britain and France, to turn the Soviet Union against Germany (Ataöv, 1965, pp. 62-63). Molotov himself, in his speech on 31 October 1939, echoed Berlin’s assessments, accusing Türkiye of abandoning its neutrality and tying its fate to that of the Western imperialist powers (Dobrinescu-Pătroiu, ib., pp. 16-17).

The following day, during his annual speech at the opening of the National Assembly, Turkish President İsmet İnönü spoke in traditionally positive terms about the Turkish-Soviet relations (Ataöv, 1965, p.63), but, according to Romanian diplomat Gheorghe Căpităneanu, who was present at the ceremony, this time, the passage in question elicited only polite applause, unlike the passage referring to friendship with Great Britain and France, which was greeted with energetic applause and ovations (Fond 71/Türkiye, vol. 61, l. 253).

However, despite certain (maximal) interpretations regarding the commitments made by the Republic of Türkiye, on 19 October 1939, it maintained its *de jure* neutrality until 23 February 1945, and *de facto* until the end of the conflagration, constantly and successfully avoiding direct involvement in the war on the grounds of insufficient preparation of its armed forces (Biagini, 2005, pp. 126-134).

On 23 October Romanian Foreign Minister Grigore Gafencu himself conducted a survey with Soviet chargé d’affaires P. G. Kukoliev. In his discussion with the Soviet diplomat, Gafencu emphasized the common aspirations and interests of peace, security, and cooperation among the Black Sea littoral states and argued that “*a rapprochement between all the Balkan states could be in the direct interest of these countries as well as of the neighbouring Great Powers, by preventing the spread of war in this part of Europe...*” (Dobrinescu-Pătroiu, ib., p. 16). The initiative of the head of Romanian diplomacy remained without a concrete response. However, it can be said that there was an indirect response from Moscow, but it consisted of several Soviet officials and diplomats circulating statements that “*when the Romanian government is asked about Bessarabia, it will be ceded without a fight*” (RRS, II, 2003, doc. 139, p. 278).

The fact that Soviet-Romanian relations were frosty raised hopes in Budapest. Also on 23 October, Hungarian Foreign Minister Count Csáky István spoke out against joining a regional bloc initiated or supported by Romania, pointing out

that Hungary had a good chance of obtaining Transylvania in the event, considered very likely, of a joint Soviet-Bulgarian attack on Romania, in Bessarabia and Dobruja, respectively (Marzari, *ib.*, p. 782).

THE SYSTEMATIZED PROJECT STAGE

Among the Great Powers, the Soviet Union continued to have the most unfavourable attitude towards rapprochement between the states of South-Eastern Europe, even at the beginning of November 1939. On 6 November, when he was not yet familiar with the details of the Neutral Bloc project, Molotov addressed Berlin, communicating the USSR's dissatisfaction regarding the plans to establish a Balkan bloc of neutral states, and on 9 November the Soviet minister in Sofia, Anatoli I. Lavrentiev, declared that the USSR would never allow Italy to lead a Balkan bloc (Marzari, *ib.*, p. 784). In contrast, the German ambassador in Ankara, Franz von Papen, in discussions held around the same time with his Romanian counterpart, Vasile Stoica, did not object to the idea of a neutral bloc with Italy's participation, but he expressed skepticism about Turkiye, which he described as "*almost belligerent*" by virtue of the agreements concluded with France and Great Britain; in response, the Romanian diplomat recalled the situation of Italy, considered similar to that of Turkiye, but in the sense of a special relationship with Germany (Ekrem, 1993, pp. 108-109).

Following the Soviet initiative of 6 November, German foreign policy leaders approached Rome, suspecting possible secret negotiations between Italy and the Balkan states. Consequently, on 16 November 1939, Mussolini and Ciano reiterated to the German ambassador in Rome the statements they had made a month earlier, but still without making any public announcement (Marzari, *ib.*, pp. 785-786).

Meanwhile, through Turkiye, the Soviet government had become aware of the full content of the Romanian diplomatic project. On 11 November Numan Menemencoglu had communicated this content to Soviet Ambassador Aleksei Terentiev, along with the information that the Turkish ambassador to the USSR, Ali Haydar Altay, had been tasked with informing the Soviet government about this Romanian diplomatic initiative (DVP, II, 1992, doc. 768, pp. 278-279, strictly confidential telegram).

On 13 November, V. M. Molotov questioned the German ambassador, Friederich Werner von der Schulenburg, about the surveys undertaken by Romania with a view to forming a bloc of neutral countries; according to the information held by Molotov, Grigore Gafencu had claimed that he already had the agreement of Great Britain, France, Italy, and even Germany. In response, the German ambassador attributed

this alleged statement by Gafencu to his tendency to mistake his wishes for reality and estimated that Bulgaria, Hungary, Greece, and Yugoslavia were not interested in the project, while Italy's position was unknown and that of Germany was unspecified (Ib., doc. 773, pp. 285-287). On 17 November, in a new conversation, Molotov and Schulenburg again addressed, this time among several other topics, the issue of the Romanian diplomatic initiative. The Reich representative stated that he had informed the Berlin government about Molotov's communications four days earlier, receiving only a preliminary response at that time, that the German government was still waiting, and that Gafencu's statements about the positive opinion from Wilhelmstrasse were premature, to say the least (Ib., doc. 790, p. 314).

Later, Joachim von Ribbentrop would assure Moscow that both powers of the Berlin-Rome Axis opposed the Gafencu plan, which was considered favourable to Great Britain and France, as it would allow them to consolidate their positions in the Black Sea, also to the detriment of the Soviet Union (Marzari, ib., p. 785). During November 1939, the Soviet Union continued its policy of pressure on the two non-Slavic neighbouring countries on the Black Sea, Romania and Türkiye.

According to the estimates of the Japanese ambassador in Moscow, quoted by Gheorghe Davidescu in a telegram sent on the first day of November, the concentration of Soviet troops near the Romanian borders did not have “*a direct and immediate purpose*”, but rather the Soviet government was waiting for either a favourable moment or a pretext to take action, for example, a possible crossing of the Straits by the British and French military fleets (Lungu, Negreanu, ib., doc. 26, p. 198).

On 3 November, during meetings between the Romanian foreign minister and the French ambassador and British minister plenipotentiary in Bucharest, Adrien Thierry and Reginald Hoare, respectively, it became clear that, in practical terms, the two Western powers had no concrete means of providing military assistance to Romania in the event of aggression by the USSR. (Ib., doc. 28-29, pp. 199-203). Finally, in mid-December, Great Britain officially informed the Romanian government that the application of the guarantees of 13 April 1939, in the event of Soviet aggression, was conditional on the attitude of Italy and Türkiye (Ib., doc. 33, pp. 209-211), which was basically a negative response to Romania's requests on that issue, given the “*Russian clause*” in the Anglo-Franco-Turkish treaty of 19 October 1939. In fact, at the end of November 1939, Richard A. Butler told I. M. Maiski that the fate of Bessarabia was of no interest to the British Empire, which wanted to collaborate with the USSR in order to stop German expansion towards the Black Sea (Sturza, editor, 2016, pp. 258-259).

As early as 4 November, the Romanian government had approached the German government with a view to mediating negotiations that would lead to an improvement in relations, and even to the conclusion of a non-aggression pact between Romania and the Soviet Union (Hayness, 2003, p. 130). At the same time, rumours were spreading in various diplomatic circles that, after the conclusion of the Soviet-Finnish negotiations that began in early October, the Kremlin would take action on the issue of Bessarabia (Constantiniu, 2002, p. 110, note 4; Lungu, Negreanu, *ib.*, doc. 30, pp. 203-204).

Towards the end of November, the USSR attempted to resume talks with Türkiye on the conclusion of a mutual defense pact, but the Ankara government made the resumption of discussions conditional on the withdrawal of the two Soviet demands that had been rejected by Şükrü Saracoğlu during the talks in Moscow, namely the amendment of the Montreux Convention and the introduction of a “*German clause*” in the text of the future bilateral treaty (Ekrem, 1993, p. 111).

Almost simultaneously, in issue 10 of the Comintern magazine for 1939, an article entitled “*The Imperialist War and Romania*” appeared, signed by the first secretary of the Communist Party of Romania, Boris Ştefanov (an ethnic Bulgarian from Southern Dobruja), written on 24 November. The basic idea of the text was that the only salvation for Romania and “*its peoples*” would have been, supposedly, the urgent conclusion of a mutual assistance pact with the USSR, following the model of Estonia, Latvia, and Lithuania. Many diplomats and politicians saw the publication of this article as a sign that the USSR was preparing to apply the “*Baltic method*” to Romania as well (Constantiniu, 2002, pp. 94-95). In some Berlin circles, there was a piece of “*information*” circulating that a Soviet attack on Romania was to take place on 6 December (*Ibid.*, p. 95). Meanwhile, however, at the end of November, the “*Winter War*” broke out between the USSR and Finland, and the unexpectedly strong resistance of the Finns to Soviet aggression prompted the Kremlin to postpone its plans for Romania and South-Eastern Europe. On 8 December, Molotov in Moscow and Pavel G. Kukoliev in Bucharest made statements distancing themselves from the ideas in Boris Ştefanov’s article (*Ib.*, pp. 95-96).

The two great Western democratic powers at war with Germany, namely Great Britain and France, had communicated their favourable opinion of the project in the first half of November, which most likely led to Berlin’s ultimately unfavourable attitude.

London’s positive and unreserved opinion was communicated on November 6 (IPERD, 2003, p. 320), while in Paris there were still some uncertainties, particularly

regarding Rome's role in this planned regional constellation. The French ambassador in Paris, R. Massigli, expressed a series of suspicions on this subject at the beginning of November, and the positive opinion communicated to Grigore Gafencu by Adrien Thierry on 13 November contained some reservations generated by the Quai d'Orsay's fears regarding Italy's supremacy within the planned bloc of neutral states (Tudorancea, 2011, p. 162). Also, in response to French objections regarding Italy's role in his regional political project, Grigore Gafencu asked the Romanian ambassadors in Ankara, Athens, and Belgrade in early November to insist on two points: 1. Only Italian participation was likely to have a positive effect in Budapest and Sofia. 2. This participation had every chance of strengthening Italy's neutrality in the long term (Ekrem, *ib.*, p. 110).

However, Romania's military attaché in Rome, Colonel Gheorghe Petrescu, assessed in a report drawn up on 31 October that the chances of attracting Italy into a regional anti-Soviet defensive bloc were null and void, since, in the Romanian officer's view, such a move would have led to tension in Rome's relations with Moscow and deepened the rift in the relations with Berlin, thus ultimately bringing Italy closer to London and Paris, which was not at all in the intentions of the Italian fascist leaders (Apud Dobrinescu-Pătroiu-Nicolescu, 1999, pp. 247-248). In the same comprehensive summary report, Colonel Petrescu mentioned that he constantly received assurances from his Soviet counterpart regarding the USSR's most peaceful intentions towards Romania, including the absence of any territorial claims (*ib.*, p. 248). The reactions of the Balkan Entente member states were essentially favourable, but official affirmative responses would not be issued until the third week of December, after the project had been definitively abandoned.

The first allied government to be officially consulted was Greece. On 30 October, Romanian Ambassador Radu Tr. Djuvara was received by General I. Metaxas and Nikolaos Mavroudis (Undersecretary of State for Foreign Affairs). The two expressed interest and promised a firm response for the following week (Tudorancea, 2011, p. 162). At the same time, in the following months, Greek diplomacy expressed its willingness to contribute to the improvement of Turkish-Italian relations (Ekrem, *ib.*, pp. 107-108).

On 31 October, legation counselor Gheorghe Căpităneanu had a discussion with the head of Turkish diplomacy, Şükrü Saracoğlu. According to the Romanian diplomat's telegram, the Turkish foreign minister had expressed a favourable attitude towards the project, but this was overshadowed by a certain distrust of Bulgaria's intentions, the conclusion being that laborious negotiations would follow.

Surprisingly (and unrealistically), Italy's attitude was considered favourable, and Rome's dissatisfaction with the act of 19 October was minimized. (RPMRROT, II, 2024, doc. 73, pp. 203-204). In the case of Türkiye, consultations with the French and British allies followed (Cojocaru, 2014, p. 207), but also, as we have shown, the Soviets were informed.

On 5 November, Gafencu was still optimistic, awaiting responses or counterproposals from Ankara, Athens, and Belgrade (Dobrinescu-Nicolescu-Pătroiu, 1999, p. 248).

Within the Balkan Entente, Romania's relations with Yugoslavia (increasingly "equidistant" between the Great Powers, and increasingly distant from its traditional and regional allies) had become quite problematic. As early as 15 July, the Romanian military attaché in Belgrade, Lieutenant-Colonel Gheorghe Popescu, had sent a report on the increasingly cold, even hostile attitude of Yugoslav public opinion towards Romania, in contrast to the increasingly friendly attitude towards Bulgaria and even Hungary, visible both in public opinion and at the official level (Collection XIV, dossier 278, II. 210-213).

On 10 November 1939, Ambassador Victor Cădere met with the head of Yugoslav diplomacy, Aleksandar Cincar Marković, to discuss the Neutral Bloc project. The Yugoslav official initially presented the results of the surveys conducted among the ministers of Great Britain, France, Germany, and Italy in Belgrade (Yugoslavia had no diplomatic relations with the USSR). The French and British ministers were in favour of the project, the German minister had some objections to Türkiye's participation in the project, while the Italian minister was skeptical because of the tensions between the Balkan states. For his part, Marković stated several conclusions, namely that Italy's participation was indispensable for the establishment and functioning of the Bloc, but that Italy remained reserved, and that clarification was needed between Italy and Türkiye, as well as a détente in relations with Hungary and Bulgaria. In turn, at the end of the telegram sent to Bucharest, the Romanian diplomat summarized some of his Yugoslav counterpart's more convoluted assessments in the following formula: *"If sacrifices were to be made for the establishment of the Bloc, they should be made only by Romania."* (Fund 71/Yugoslavia, vol. 52, II. 221-223).

Yugoslavia's distancing from the other Balkan Entente states continued. Thus, on 13 November the Yugoslav General Staff notified its counterparts in Romania, Greece, and Türkiye of its (unilateral!) decision to cancel the annual meeting of the chiefs of staff of the four allied countries, planned to take place

in Belgrade at the end of 1939 (Ibid., I. 228). At the same time, the Romanian General Staff, through its chief, General Florea Țenescu, informed the Ministry of Foreign Affairs on 27 November that the Yugoslav side had not sent the Romanian side a response to the draft bilateral (secret) military convention against Hungary and Bulgaria, which had been submitted to it in August (Ibid., I. 229).

The small revisionist states neighbouring Romania, Bulgaria and Hungary, once again expressed their revisionist aspirations and disinterest in initiatives based on the territorial status quo in the context of the promotion of regional cooperation plans.

Thus, in discussions on 10 and 20 November with Romanian Minister Eugen Filotti in Sofia, Gheorghe Kyosseivanov rhetorically asked who the future bloc of neutral states was directed against, given that Germany had given assurances considered credible in terms of keeping the Balkans out of the conflict, and on 5 December, in an interview with the newspaper *Paris Soir*, he reiterated the idea of Bulgaria returning to its pre-Second Balkan War borders (Ungureanu, 2009, pp. 347-348). The radio address of 26 November by the new Romanian Prime Minister, Gheorghe Tătărescu, referring, among other things, to the defense of his own borders and mutual concessions on the issue of minorities, was harshly criticized by the Bulgarian press (Ib., p. 348).

On 11 November, alarmed by the appearance in the Bulgarian press of articles taken from the Italian press concerning the creation of a regional bloc of neutral states under the aegis of Italy, the Soviet minister in Sofia, A.I. Lavrentiev, requested an audience with Gheorghe Kyosseivanov for clarification on this issue. According to the Soviet diplomat, who had certain doubts about the sincerity of his interlocutor, the latter made the following statements and assessments:

- The Neutral Bloc was an anti-Soviet project;
- The implementation of this project would have led to war in the region, given Türkiye's position after 19 October;
- Bulgaria would maintain its neutrality and freedom of action;
- Bulgaria's minimal aspirations were to return to the borders of (spring) 1913;
- There were no indications of Italian interest in organizing a regional bloc of neutral states;
- If Bulgaria were to receive concrete official proposals to join such a bloc of states, the Soviet government would be promptly informed (DVP, II, 1992, doc. 771, pp. 281-282).

A new meeting between Kyosseivanov and Lavrentiev took place on 15 November. According to a strictly confidential telegram sent by the Soviet diplomat to Moscow, the head of the Sofia government thanked the Soviet government for its attitude towards Bulgaria and its aspirations, pointed out that joining a neutral Balkan bloc was not in Bulgaria's interest, and specified that Germany was opposed only to Türkiye's presence in such a structure (Ib., doc. 783, pp. 298-299). The Hungarian reaction was even more categorical. After being assured that Italy was not interested in the Romanian project, Count Csáky began to sabotage it by putting forward and circulating demands that were impossible to meet. Thus, in a speech on 21 November, the Hungarian foreign minister made clear references to Transylvania, but also allusions to the Romanian diplomatic initiative, based on the frontiers that were considered "*unjust*" in Budapest (Marzari, ib., p. 783).

Towards the end of November, Moscow's opposition, which had also intervened in Berlin, on the one hand, and Italy's implicit disinterest, on the other, as well as negative reactions from Sofia and Budapest, converged towards the failure of the Neutral Bloc project.

On 28 November, Grigore Gafencu told the German minister in Bucharest, W. Fabricius, that, given the objections from Italy and Germany, the Neutral Bloc project had just been abandoned (Hayness, 2003, p. 128). A similar communication had been made by the head of Romanian diplomacy to the Italian chargé d'affaires, Capece, three days earlier (Marzari, ib., p. 786).

On 29 November, Grigore Gafencu gave a presentation at the Senate headquarters before the Foreign Affairs Committees of both Chambers. With regard to the USSR, the head of Romanian diplomacy spoke once again about the mutual advantage of good-neighbourly bilateral relations, beyond differences in ideology and internal political regime, and reiterated references to the Moscow Protocol (9 February 1929), the London Conventions (3-5 July 1933), and other instruments of international law adopted by both states (RRS, II, 2003, doc. 141, pp. 280-281, note 1). However, V. M. Molotov's assertions at the end of October regarding the alleged obsolescence and inadequacy of old concepts of international law, such as "*aggressor*" and "*aggression*", seriously called into question Gafencu's optimistic tone, and the USSR's conduct towards Finland only served to confirm, once again, the lack of practical value of the obligations previously assumed by the Soviet state.

At the beginning of December, however, new reasons for hope emerged for Romanian diplomats, linked in particular to certain attitudes of Italy towards the Soviet Union and towards South-Eastern Europe, in the context of the unexpectedly strong resistance of the Finns to the Red Army.

Turkish Foreign Minister Şükrü Saracoğlu also expressed a certain optimism regarding Italy on 2 December 1939, in a discussion with Romanian Ambassador Vasile Stoica. According to the Romanian diplomat’s account, Turkish-Soviet relations remained quite cold, with Turkish public opinion outraged by the aggression against Finland. Saracoğlu did not believe in the concrete possibility of forming a bloc of neutral states capable not only of maintaining their neutrality, but also of repelling a possible aggression, due to a complex set of obstacles, namely the positions of Germany, the USSR, Hungary, and Bulgaria, and even the attitude of Yugoslavia. However, the head of diplomacy in Ankara did not believe in the durability of the German-Soviet partnership either (RPMROT, II, 2024, doc. 76, pp. 240-241). On 4 December, Gafencu addressed Ciano, through the Italian diplomat Capecece. Ciano’s response arrived on 7 December, and was essentially categorically negative, beyond some generalities regarding Italy’s sympathy for attempts to improve relations between the Balkan states, which led Grigore Gafencu, on 9 December, to definitively acknowledge the failure of the project (Marzari, 1970, pp. 786-787).

The article *“Us and the Others: Italy and the Balkan Balance”*, published in the 5 December 1939 issue of the daily newspaper *Il Messagero*, caused quite a stir in European diplomatic circles. The article began by noting the existence or persistence of two trends in the Balkans, namely Pan-Slavism and Pan-Germanism, to which, after the events of April 1939 (the annexation of Albania), the assertion of Italian influence had been added. According to the Italian newspaper, this more recent trend did not contradict German interests, but rather Soviet and Bolshevik expansionist tendencies (Collection XIV, dossier 197, I. 25-28).

The article quoted above was also interpreted as an implicit Italian response to Boris Ştefanov’s article, *“The Imperialist War and Romania”*. The direct and unfavorable reaction of the Italian press to the article authored by the aforementioned communist leader was, in fact, particularly energetic, a fact that was received with satisfaction in Romanian circles (Dobrinescu-Pătroiu-Niculescu, ib., pp. 256-257). Departing from its previously rather reserved attitude, the press on the peninsula showed unusual solidarity with the Romanian state, unanimously condemning Boris Ştefanov’s assertions, which were seen as a symptom of the USSR’s territorial and ideological expansionist tendencies in the Balkans, while also highlighting Italy’s interests in the Balkans and its role as a counterweight to the Bolshevik threat. The *Gazzeta del Popolo* of 9 December 1939 went so far as to attribute the official Soviet denials and delimitations from Ştefanov’s article to Italy’s firm anti-Bolshevik attitude, manifested in the communiqué of the Fascist Grand Council of 5 December (ib., pp. 22-23).

This attitude on the part of the Italian press, which would have been impossible without the consent of the fascist authorities, as well as certain passages in the communiqué of the Grand Council of Fascism, created exaggerated hopes in certain Romanian circles. Thus, a military document dated 11 December 1939, entitled *"How Italy's commitments in South-Eastern Europe are being discussed in diplomatic circles"* and marked *"Censored from the press"*, ended with the completely unrealistic conclusion that the regime in Rome had just sent a signal for the resumption of efforts to establish a bloc of neutral states (Ib., I. 31).

On 8 December, two Romanian-Soviet diplomatic contacts took place, namely the meeting between Gr. Gafencu and P. G. Kukoliev in Bucharest, and the meeting between Vladimir Petrovici Potëmkin and Gheorghe Davidescu in Moscow.

According to the meeting notes taken by Gafencu, the head of Romanian diplomacy assured his Soviet guest of Romania's peaceful intentions towards the USSR, but his interlocutor was not very impressed, complaining that various Romanian circles were spreading the idea of a *"Soviet threat"*, which he claimed was unfounded (RRS, II, 2003, doc. 141, pp. 280-282). According to the Soviet version, a significant part of the discussions was devoted to the subject of the *"Balkan bloc"*, with Kukoliev repeatedly expressing his suspicions about Italy's invitation and, in particular, about *"its insistent desire to be part of the bloc"*, a desire clearly proven, in the view of the chargé d'affaires of the USSR, by the communiqué of the Fascist Grand Council (Ib., doc. 143, pp. 284-285).

According to the telegram sent by Gheorghe Davidescu also on the evening of 8 December 1939, the discussion that same day with V. P. Potëmkin had lasted about 25 minutes. The deputy head of Soviet diplomacy expressed his disapproval of Ștefanov's article, but did not show much interest in Gafencu's statements regarding the convergence of Romanian-Soviet interests in the Black Sea and evaded a concrete answer regarding the start of negotiations for the conclusion of a bilateral trade treaty, despite Davidescu's insistence on both issues, especially the latter. The only subject in which Potëmkin showed a certain interest, which he tried to mask, was the one regarding obtaining translations of Grigore Gafencu's latest statements on the Balkan bloc issue (Ib., doc. 142, pp. 282-284).

It is not insignificant that three days earlier, during a meeting with the French ambassador to the USSR, Paul-Emile Naggjar, the same V.P. Potëmkin stated that *"Bessarabia is the true natural agricultural hinterland for Odessa"*, and that the Soviet government would raise the issue of Bessarabia *"if the fighting in Finland ends quickly"* (Oprea, 2003, p.199).

In the first half of December 1939, several signals arrived in Bucharest from German sources, indicating that the Reich could not prevent the occupation of Bessarabia by the USSR, but that it could not allow the Sovietization of larger areas of Romania, let alone the entire country, as outlined in the scenario put on paper by Boris Ștefanov (Hayness, 2003, pp. 130-131). Thus, on 13 December the chargé d'affaires for economic affairs for South-East Europe, Carl Augustin Clodius, told General Ernest Urdăreanu that Germany could support Romania against a Soviet attack under certain conditions, but only if the Red Army crossed the Prut River (Oprea, 2003, p. 195). Responding to a telegram sent from Bucharest by W. Fabricius on 8 December, which mentioned Gafencu's hope for diplomatic action by Germany to improve Romanian-Soviet relations, Ernst von Weizsäcker stated on 15 December that Berlin's interest was for Romania to make certain territorial concessions to the Soviet Union by peaceful means, so as to avoid the outbreak of war (Sturza-editor, 2016, pp. 259-263).

A similar view was held by the Italian ambassador to Moscow, Augusto Rosso, who, on 10 December declared to his North American counterpart, Laurence Adolph Steinhardt, that Italy would most likely not react, in the event of a Soviet attack on Romania, to obtain (only) Bessarabia, but *“Any attempt by the USSR to penetrate further into the Balkans, or along the Black Sea, would be met with Italian opposition, even by force of arms.”* (Ib., pp. 261-262). The attitude of the Yugoslav ally was not too favourable to Romania this time, either. Thus, on 7 December 1939, very upset by the text of the article signed by Boris Ștefanov, the Yugoslav minister in the capital of Great Britain, Ivan Subotić, visited the Soviet ambassador I. M. Maiski. The conclusion of what the Yugoslav diplomat had said, not explicitly formulated by him, but drawn by the Soviet one and communicated the next day in Moscow, was as follows: *“Take Bessarabia, but slowly, so that no war breaks out in the Balkans!”*. In reply, Maiski assured him that the Soviet Union also wanted to avoid “unnecessary complications” (Ibid., p. 259).

On 11 December, Pavel G. Kukoliev reported on the intensification of Romanian fears regarding the USSR following the outbreak of hostilities in Finland, a development he attributed to the British. In this context, the Soviet diplomat also mentioned that Romania's defensive military forces in the East were concentrated on the Prut River, not on the Dniester River or inside Bessarabia (RRS, II, 2003, doc. 144, pp. 285-288). On the same day, Gh. Davidescu sent a report from Moscow. The Romanian diplomat was aware that the Soviet Union had only postponed its action against Romania, but he had some hopes, linked to the Red Army's poor

military performance on the Finnish front and its possible long-term consequences (Lungu, Negreanu, ib., doc. 32, pp. 206-209).

The first official positive response to the proposals put forward by Gafencu at the end of October came from Athens on 16 December (Tudorancea, 2011, p. 163), exactly on the day when Galeazzo Ciano made public, in Rome, Italy's lack of interest in this project. On 18 and 21 December, respectively, positive responses also arrived from Ankara and Belgrade (Dobrinescu-Pătroiu-Nicolescu, ib., p. 249). However, the project was no longer relevant in Bucharest, as the negative positions of Moscow, Berlin, Rome, Sofia, and Budapest were already known.

EPILOGUE

After the failure of the *"Neutral Bloc"* project, Romanian diplomacy continued, until the spring 1950, to pursue, separately, the objectives that had been the basis of the project systematized towards the end of October 1939.

The USSR continued to be perceived as the greatest threat to the Romanian state and, first of all, to its territorial integrity. A negative element in bilateral relations occurred on 14 December 1939, when Romania voted in favour of the proposal to exclude the Soviet Union from the League of Nations, following the aggression against Finland (IPERD, 2003, p. 320). On the same day, Grigore Gafencu sent a circular telegram to Romania's diplomatic representatives in Paris, Berlin, Ankara and Budapest. The head of Romanian diplomacy recommended increasing contacts with Soviet representatives, for two purposes, namely deciphering Moscow's intentions towards Romania, and also explaining Romania's peaceful intentions towards its great neighbour to the east and north (RRS, II, 2003, doc. 145, p. 289).

At the end of 1939, it had become obvious to the leadership of Romanian diplomacy that Great Britain and France would not support Romania in the event of a Soviet attack. The greatest hopes for such a scenario continued to be linked to Italy. Moreover, in the winter of 1939-1940, in the conditions of the Soviet-Finnish war, diplomatic relations between Italy and the USSR experienced a historic crisis, leading to the prolonged withdrawal of the two ambassadors from their posts for consultations (Constantiniu, 2002, p.76).

In the spring of 1940, after the end of hostilities in Finland, the interest of the USSR in the Balkans became more visible, an important moment being the well-known speech of V. M. Molotov on 29 March 1940. Almost a month later, in a summary report for the period 24 March–24 April 1940, the Romanian military attaché in Rome, Lieutenant Colonel Gheorghe Petrescu, noted a series of changes

in the Italian foreign policy discourse, first of all, an *“intense propaganda action, intended to prepare the ground for entering the war alongside Germany”*, but also a softening of the tone towards the Soviet Union. *“There is no longer a single word, however slightly offensive, in the entire Italian press against our Eastern neighbour. The speech of Mr. Molotov, whp officially put the issue of Bessarabia back on the agenda, was not the subject of any kind of comment in the Italian press and was simply recorded.”* (Collection XIV, dossier 278, ll. 246-273). So, a major change compared to December 1939 and the reaction to Boris Ștefanov’s article.

Indeed, on 10 June 1940, Italy joined Germany in the war, and Italian-Soviet relations emerged from the frosty period that had largely corresponded to the calendar winter of 1939-1940. This development in relations between Rome and Moscow was tacitly based on the idea expressed directly by Molotov on 20 June 1940, in a discussion with Ambassador Augusto Rosso, who had since returned to his post: *“The Soviet government recognizes Italy’s supremacy in the Mediterranean, provided that Italy also recognizes the Soviet Union’s supremacy in the Black Sea.”* (Simion, 1996, pp. 165-166). A few days later, Bessarabia and other Romanian territories were seized.

Cooperation within the Balkan Entente also failed to make any notable progress in the first half of 1940. The last meeting of the Balkan Entente Council, held in Belgrade between 2 and 4 February 1940, highlighted the deepening differences between member states, especially between Türkiye and Yugoslavia, beyond the unanimous, but practically formal, to extend the Balkan Pact for seven years (Oșca, 2024, pp. 234-235, 251). Military cooperation within the Balkan alliance was practically blocked, with Yugoslavia’s conduct, especially the organization of its military forces in Western Banat, coming to be viewed with suspicion by the higher echelons of the Romanian army in the spring of 1940 (Ib., pp. 256-258). Nor was Romanian-Turkish military cooperation functioning within the previously agreed parameters any longer, and a meeting of the chiefs of staff of the four allied states, scheduled, in principle, in Athens, for mid-1940, never took place (Fond 71/Türkiye, vol. 61, pp. 286, 306-309).

Bulgaria’s interest in joining an increasingly dysfunctional regional alliance based on the territorial status quo was also practically nil, the rulers in Sofia deciding, on 4 April 1940, to launch a vast diplomatic campaign regarding Southern Dobruja and to categorically express their territorial claims towards Romania immediately after Italy or the USSR had taken action in this part of Europe (IID, T2, 1993, part two, doc. 49, pp. 370-371). That moment came at the end of June 1940.

Meanwhile, at the end of May, Grigore Gafencu had left the leadership of Romanian diplomacy, entrusted by King Charles II to Ion Gigurtu, a well-known Germanophile.

CONCLUSIONS

The Romanian initiative of the “*Neutral Bloc*” in the autumn of 1939 represented an attempt by Romanian diplomacy to limit the proportions of the Soviet threat (amplified after 23 August 1939) by uniting the states of South-Eastern Europe, especially Italy, relying on a supposed Italian-Soviet antagonism in this part of Europe.

The project was not in itself anti-Soviet, except in so far as the USSR had expansionist ambitions in the area, and highlighting peaceful intentions towards the Soviet Union remained a priority for Romanian diplomacy during this period. However, Moscow was not interested in maintaining the regional status quo, so that, of the Great Powers of the time, the USSR reacted most promptly and most negatively to the Romanian diplomatic initiative, also drawing in Germany, which initially had expressed only certain reservations, mainly related to the role of Türkiye, a state with close relations with Great Britain and France, both enemies of the Reich.

With regard to Italy, Romanian diplomacy overestimated that country’s willingness and ability to oppose Soviet territorial and ideological expansion in the Balkans and to maintain its neutrality. This was also contributed to by the rhetoric of Italian diplomacy and the press, in particular the belated announcement of Italy’s unwillingness to participate in any regional political-military bloc of neutral states, even though the decision to this effect had been taken as early as 17 October, allowing Grigore Gafencu, Romania’s foreign minister, to finalize the “*Neutral Bloc*” project. The fact remains remarkable that Romania’s military attaché in Rome, Lieutenant Colonel Gheorghe Petrescu, managed to decipher the guidelines of Italian foreign policy very well, both in the autumn of 1939 and in the spring of 1940.

The attitude of Moscow, Berlin, and Rome towards Gafencu’s project, and, by extension, towards the idea of forming a regional bloc of neutral states, dashed any hopes of Sofia and Budapest joining in, leading to the failure of this ambitious Romanian diplomatic initiative.

In turn, this failure highlighted the growing isolation of the Romanian state at the regional level, especially when corroborated with certain signals received from various European capitals on the issue of Bessarabia.

However, despite the failure, Romanian diplomacy maintained the same general lines of action in the first months of 1940, in relation to the belligerent Great Powers, Italy, the USSR, the allied Balkan states, respectively Bulgaria and Hungary, until, under the pressure of new changes in the international context (the reaffirmation of Soviet claims over Bessarabia, the Italian-German rapprochement, the evolution of hostilities in Western Europe), the option of rapprochement with the Reich would become predominant.

However, despite the failure, Romanian diplomacy maintained the same general lines of action in the first months of 1940, in relation to the belligerent Great Powers, Italy, the USSR, the allied Balkan states, respectively Bulgaria and Hungary, until, under the pressure of new changes in the international context (the reaffirmation of Soviet claims over Bessarabia, the Italian-German rapprochement, the evolution of hostilities in Western Europe), the option of rapprochement with the Reich would become predominant.

BIBLIOGRAPHY:

1. Ataöv, T. (1965). *Turkish Foreign Policy 1939-1945*, Ankara: Ankara University Publishing House.
2. Biagini, A. (2005). *Istoria Turciei contemporane/History of Contemporary Türkiye*, translation by Ioana Mândrescu, Cluj-Napoca: Accent Publishers.
3. Cliadakis, H. (1974). *Neutrality and War in Italian Policy 1039-1940*, in “*Journal of Contemporary History*”, vol. 9, no. 3, pp. 171-190.
4. Cojocaru, I. (2014). *România și Turcia, actori importanți în sistemul de relații interbelice (1918-1940)/Romania and Türkiye – Important actors in the interwar system of relations (1918-1940)*. Târgoviște: Cetatea de Scaun Publishing House.
5. Constantiniu, Fl. (2002). *1941. Hitler, Stalin și România. România și geneza operațiunii „Barbarossa”/Hitler, Stalin and Romania. Romania and the genesis of Operation “Barbarossa”*. Bucharest: Corint Publishing House.
6. Dobrinescu, V. Fl., Pătroiu, I. (1992). *Anglia și România între anii 1939-1947/England and Romania between 1939 and 1947*. Bucharest: Didactic and Pedagogical Publishing House.
7. Dobrinescu, V. Fl., Pătroiu, I., Nicolescu Gh. (1999). *Relații politico-diplomatice și militare româno-italiene (1914-1947)/Romanian-Italian political, diplomatic and military relations – (1914-1947)*. Pitești-Craiova: Intact Publishing House.
8. DVP (1992). *Dokumenti vneshney politiki, 1939 god., kniga vtoraya 1 septyabrta – 31 dekabrya 1939 god/Foreign Policy Documents, 1939, Book Two, September 1 – December 31, 1939*. Moscow: Ministry of Foreign Affairs of the Russian Federation.
9. Ekrem, M.A. (1993). *Relațiile româno-turce între cele două războaie mondiale (1918-1944)/Romanian-Turkish relations between the two world wars (1918-1944)*. Bucharest: Scientific Publishing House.

10. Genchev, N. (1998). *Vănsnata politika na Bălgariya (1938-1941)/The Foreign Policy of Bulgaria (1938-1941)*. Sofia: Vektor Publishers.
11. Haynes, R. (2003). *Politica României față de Germania (1936-1940)/ Romania's policy towards Germany (1936-1940)*, translation by Cristina Aboboaie. Iași: Polirom Publishers.
12. IID (1993). *Izvori za istoriata na Dobrudja 1919-1941/Sources for the History of Dobrudja 1919-1941*, editor-in-chief: Petur Todorov, contributors: Petur Todorov, Kosyo Penchikov, Marin Tsutsov, Stela Izvorska, Antonina Kuzmanova. Sofia: Publishing House of the Bulgarian Academy of Sciences.
13. IPERD (2003). *Istoria politicii externe românești în date/The History of Romanian Foreign Policy in Dates*, I. Calafeteanu editor. Bucharest: Encyclopedic Publishing House.
14. Lungu, C.M., Negreanu I. Al. (2000). *România în jocul Marilor Puteri (1939-1940). Documente (1938-1941)/Romania in the game of the Great Powers (1939-1940). Documents (1938-1941)*, with an introduction by Dinu C. Giurescu. Bucharest: Curtea Veche Publishing House.
15. Marzari, F. (1970). *Projects for an Italian-led Balkan Bloc of Neutrals, September-December 1939*, in „*The Historical Journal*”. Cambridge University Press, vol. 13, no. 4, pp. 767-788.
16. Oprea, I.M. (2003). *România și Imperiul Rus. Volumul al II-lea (1924-1947) / Romania and the Russian Empire. Volume II (1924-1947)*. Bucharest: Albatros Publishing House.
17. Oșca, Al. (2024). *Pactul Balcanic. Acțiune diplomatică și cooperare militară/The Balkan Pact. Diplomatic Action and Military Cooperation*. Bucharest: Ștefanida Publishing House.
18. Romanian National Military Archives – “General Grigore Constandache” Central Archive Depository – Pitești. Fund Collection XIV (Studies and earches concening the Romanian Army).
19. Romanian Ministry of Foreign Affairs Archives. Fund 71/Türkiye (1920-1944).
20. Romanian Ministry of Foreign Affairs Archives. Fund 71/Yugoslavia (1920-1944).
21. RPMROT (2024). *Relații politice și militare româno-otomano-turce 1878-1989. Documente, vol. II 1939-1989/Romanian-Ottoman-Turkish political and military relations 1878-1989. Documents, vol. II 1939-1989*, coord.: Carmen-Sorina Rîjnoveanu, volume editor: Manuel Stănescu. Bucharest: Institute for Political Studies of Defense and Military History.
22. RRS (2003). *Relațiile româno-sovietice. Documente. Vol. II. 1935-1941/ Romanian-Soviet Relations. Documents. Vol. II. 1935-1941*, published by the Ministry of Foreign Affairs of Romania and the Ministry of Foreign Affairs of the Russian Federation. Bucharest: Romanian Cultural Foundation Publishing House.
23. Simion, A. (1996). *Dictatul de la Viena/The Vienna Award*, edited by Elisabeta Simion. Bucharest: Albatros Publishing House.
24. Stănciugel, R. (2008). *Lumea balcanică în misiunea și activitatea diplomatului Vasile Stoica/The Balkan world in the mission and activity of diplomat Vasile Stoica*. Bucharest: Colias Publishing House.

25. Sturza, V. (2016). *Basarabia și destinul ei secret. Mărturii și documente istorice/ Bessarabia and its secret destiny. Testimonies and historical documents*. Bucharest: Litera Publishing House.
26. Tudorancea, R. (2011). *Relațiile româno-elene în perioada interbelică. Dimensiunea politică și economică/Romanian-Greek relations in the interwar period. Political and economic dimensions*, with a preface by Academician Florin Constantiniu. Bucharest: Omonia Publishing House.
27. Ungureanu, G. (2009). *Problema Cadrilaterului în contextul relațiilor româno-bulgare (1919-1940)/The Problem of the Quadrilateral in the Context of Romanian-Bulgarian Relations (1919-1940)*. Brăila: Istros Publishing House.
28. Ungureanu, G. (2024). *Political-diplomatic regroupings and military implications at the Black Sea (February-October 1939)*, in *Proceedings of the International Scientific Conference “Romanian Military Thinking”*, 6th edition. Bucharest, Defense Staff, November 2024, pp. 768-795.

THE LAST STAGE OF THE CRIMEAN EVACUATION: FRICTIONS BETWEEN THE ARMY AND THE NAVY

Dr. Dan-Dragoș SICHIGEA

Department Chief at the Romanian National Naval Museum, Constanța

DOI: 10.55535/RMT.2025.3.41

At the beginning of May 1944, the German 17th Army, with its German and Romanian troops, was in a tight spot, stuck in defending Sevastopol. It was quite clear at that time that soon it would have to take another step back, in the Chersones position, the last area from where it could be extracted by sea.

This last task was assigned to Admiral Black Sea and its mixture of German-Romanian ships. The unit had already completed the first stage of the evacuation from Crimea in April 1944. In this difficult circumstances, the last stage of evacuating the stranded Axis units from the peninsula was much harder and sparked controversies among the services.

Keywords: Brinkmann; 1944; fortress of Sevastopol; Crimea; Romanian ships;

From the issuance of the order to completely stop the shipments until the completion of the first phase of the evacuation on April 27, a total of 3,973 people were transported to the West coast, of which 2,078 Romanians (A.M.N R., S.S.M., 26, f. 27). By all standards the first phase was a genuine success. Here too the sources differ and we must take into account both natural errors when counting those landed at Constanta and other ports of destination, as well as the tendency equally explainable to report the best results. The reports of the Maritime Naval Force, taken by most of the Romanian naval history volumes, give a total of 73,058 evacuees *“by sea”*, of which 20,779 Romanians and 20,494 Germans, along with 723 Slovaks and 21,302 Soviet volunteers, prisoners, civilians, etc. Compared to the modest start in terms of the number of Romanians, it is clear that the Admiral Black Sea (A.S.M.) compensated after April 20, substantially increasing the share of Romanian servicemen who were sailing on transport ships to Romania. The 17th Army reported in turn that a total of 85,836 men were evacuated with the Navy alone, plus another 16,027 by air (AOK 17, KTB no. 10, 150, f. 22). The division of evacuees according to German sources was as follows: 44,322 Germans (of whom 15,339 wounded), 29,096 Romanians (of whom 3,641 wounded). The difference between the two reports is explained by the fact that the Germans also took into account the shipments from 10-14 April, while the documents of the Romanian side start with the latter date.

Between 14-27 April there were several submarine attacks and more significantly 14 air attacks on the Axis convoys to Sevastopol. Regarding the loss of human lives, most of them were from *“Alba Iulia”* and from the barge *“Leo”*, about 500 Romanian and German evacuees. The high death toll in the case of *“Leo”* is noted, because the ship was overloaded and the enemy bombs fell in full (A.M. N.R., C.F.N.M., 33, f. 27).

The Royal Romanian and German navies in the Black Sea had reasons to be proud following the first stage of the evacuation of the Crimean bridgehead. The Naval Maritime Forces report showed that of those carried, only 0.19% had been lost. Although true, it was only one facet of the coin. The axis suffered significant losses in terms of floating material. The oil tanker *“Ossag”*, of over 2,700 tons was sunk, and three other important transport ships, *“Alba Iulia”*, *“Ardeal”* and *“Oituz”*, were taken out of action for the next stage of evacuation. *“Danubius”* was also damaged, but was still able to participate in subsequent evacuations. Of the warships, the most important blow was the damage to *“Regele Ferdinand”* on 23 April, following

repeated air attacks. Two pontoons with artillery were also damaged, and the Germans lost a transport/antisubmarine ship – “U. J. 104”, seriously damaged (A.M.N.R., C.F.N.M., 33, f. 27). It was clear both to Vice Admiral Helmuth Brinkmann, Commander of the A.S.M., and to Rear Admiral Horia Macellariu, commander of the Romanian Maritime Naval Forces, that the inevitable resumption of troop transports in Crimea would be much more difficult. If the Soviets had managed to force a retreat to the positions at Chersones their artillery would have posed serious problems at the wharves and other craft sites. On the other hand, the reduction of the transport capacity, by damaging and sinking ships, meant that the Axis had to call on military ships or organize several convoys, thus exposing itself to the dangers of Crimean waters.

Even so, on April 26 Brinkmann received the official message for A.S.M. from the Navy Command, which he also forwarded to subordinate units. Admiral Donitz remarked *“the orderly transfer of Navy personnel to Sevastopol with insignificant losses, the implementation of transport plans, the remarkable successes of commanders, General Staff, naval units and crews”* (KTB A.S.M., R 2592, c. 51). Before reaching the main idea the message praised the efforts made by the Navy in strengthening the Sevastopol bridgehead, which was justified if we take into account the fact that for a few days the line “Gneisenau” was defended by marine and Romanian units. It remained the Black Sea Fleet’s task to supply the Fortress of Sevastopol, once Hitler decided that it should be preserved because it had *“the greatest strategic importance in the broad context of the battle on the Eastern Front”* (KTB A.S.M., R 2592, c. 51). The message reinforced, therefore, for the Axis naval forces, the idea that, at least for the moment, the evacuation of troops from the peninsula was given up and the situation was returned to before April 1944 – supply convoys with men and materials for the 17th Army.

The disruption to transport was undoubtedly sudden and created big problems in turn. The order did not affect convoys that were already at sea or in the process of departing, so for several days the evacuation continued. By April 29 more than 3,000 Romanian troops arrived, most of them able men, but also over 400 Germans (A.M.N.R., S.S.M., 3055, ff. 165). The figures demonstrate unequivocally that despite the order to cease the evacuation the Romanian side continued to withdraw troops from the fortress. It is not an exaggeration to say that with the shortening of the front following the withdrawal of the Axis troops on a western alignment and leaving the exposed areas (especially in the northern sector), it was decided at the local level by the 17th Army to continue the removal from the area of the forces considered incapable of contributing to the defense of Sevastopol.

On the other hand the wounded and even some civilians and auxiliaries left in the combat zone could not be withdrawn further limiting the maneuvering space of the army in an increasingly smaller area (Koslinski, Stanescu, 1997, p. 240). Convoys carrying predominantly Romanian troops continued to suffer air and naval attacks. Such was the case with a German convoy on April 27, attacked with torpedo stars. A torpedo hit the submarine hunter "U. J. 104" at the bow, breaking a hatch and killing 50 boat soldiers below deck along with 17 crew members. Two others were seriously injured. The ship was towed to Sevastopol for repairs. Towards evening an "R-Boot" and the tugboat "Tissa", which was operating in search of a Romanian armed barge, were attacked by Soviet aircraft, which wounded two sailors (KTB A.S.M., R 2592, c. 518).

The commander of the 17th Army, General Erwin Jaenecke, could hope that his forces would be evacuated and there were good reasons for this, but he personally was not going to see the salvation of the army from the Crimean hell. His report on 27 April was sent by Schorner to the General Staff of the Army from where it reached Hitler. As a result Jaenecke was summoned to Berchtesgaden to report exactly the situation of the army and the prospects for the coming period (Buttar, 2020, p. 319). After preliminary talks with Schiffner in Galati, on 28 April, he flew to Austria to Hitler's headquarters. Although it had the support of the direct chief and that of Zeitzler, the Chief of the General Staff, Jaenecke's report could not please the German dictator as it led to the need to abandon Sevastopol. The discussions were apparently tense, especially because the arguments of the commander of the 17th Army did not convince Hitler. In turn, he promised reinforcements far from the necessary invoked by Jaenecke-instead of a division only four battalions (Ib., p. 642). In his place was appointed General Kurt Allmendinger, the former commander of the 49th Corps, who probably made a fine figure at the discussion he had had with Hitler just a few days before. Jaenecke was accused of *"no longer being fully trusted to carry out the BATTLE for Sevastopol, according to orders received"*. Allmendinger, on the other hand, enjoyed his confidence, and it could be thought, following his performance at the conference on April 25, that he would carry out the orders without much protest¹.

For its part, the Romanian Royal Navy was working feverishly on preparations for the resumption of evacuations from Crimea. The analysis of that period, regarding the possibilities in terms of available ships, concluded that in the next period one could count on five ships with large capacity – *"Ardeal"*, *"Danubius"*,

¹ KTB H.Gr. 'Südukraine', Abt. Ia, No. 3, vii. 202 ff. (21 Apr. 1944), BA-MA RH 19 V/26, fos., 203 ff., apud Klaus Schonherr, op. cit., p. 485.

“Durostor”, “Dacia” and “Romania”, which could carry in optimal conditions about 12,000 troops. The ships under the German and Hungarian flags were added, with about 20,600 more troops (A.M.N.R., fond S S.M., 3055, f. 199).

The ships represented only one dimension of the problem. As the events of the coming period will prove, the issue of Crimean boat facilities proved to be a very important factor. That is why the A.S.M. has ordered a series of measures to improve the situation on the coasts of the peninsula, anticipating of course the big problems that it will encounter in the craft of the troops. During the German occupation of Crimea, the development of port facilities both at Sevastopol and at other ports and in the bays around the city was ignored. As a result, some improvisations were required, or rather, desperate measures, such as drowning barges to be used as wharves and identifying areas for easier unloading of barges type *“M.F.P.”*. The Army was to contribute by providing bomb disposal ships, for faster unloading of steamboats at the wharves and transportation to other unloading places. As long as the large port of Sevastopol was still operational, fast tugboats could use the facilities there provided there were Army land vehicles to transport them. This possibility soon expired, however with the onset of the Soviet offensive and the retreat to Chersones (KTB A.S.M., R 2563, c. 14).

It was clear that the last variant of the evacuation conceived by Jaenecke’s general staff had to be implemented as early as April 28 – operation *“Wildkatze”* (wild cat). It is interesting to note the direction followed by the codenames given to successive 17th army response operations: from *“Tiger”* to *“Leopard”* and ending with *“wild cat”*, that is, names of felines of ever smaller size. It is somewhat natural, given the substantial diminution of the forces at the disposal of the axis in Crimea.

“Wildkatze” did not differ radically from *“Leopard”*, and the implementation of the plan meant shortening the front by withdrawing across the Severnaya Bay forces from the northern side of the line of contact with the enemy. Allmendinger decided to execute the plan on May 7 with a two-stage withdrawal the next day on May 8 and then on May 9. In parallel, in the southern sector despite the retreat to an intermediate and clearly insufficiently prepared position – the so-called Nikolaievka line, he was preparing to counterattack the Sapun Heights, captured by the Soviets. To A.S.M. and for the Crimean Naval Command (Seeko Krim) it was obvious that the loss of the coverage area north of Severnaya Bay was a heavy but anticipated blow. The loss of the Port of Sevastopol was compensated somewhat by the landscaping works, mostly improvised, in the adjacent areas. The Romanian sources correctly assess that Admiral Otto Schulz had the difficult tasks of simultaneously ensuring the transport of the 49th Corps across Severnaia,

to mine the port and to execute its destruction (Koslinski, Stanescu, 1997, pp. 248-9). His mission during the 3rd stage of the evacuation was going to be a much more difficult one no doubt. But plans for destruction and mining were being made and the fact that they were implemented very quickly was a success on itself.

Brinkmann summarizes well the situation he faced in the new circumstances in the theater of battle: *"The Port of Sevastopol is from this moment forward inoperable for our supply (unloading and loading) traffic. We have to rely from 9.5 on the outer bays, in which wharves and anchorages were arranged and in which barges were drowned. After occupying the northern coast, the enemy will cover with artillery what is left of the bridgehead, including these bays. We must expect losses of floating material due to artillery fire during port operations. If the enemy artillery will also annihilate the two remaining airfields – Sevastopol 3 and Chersones, the situation will become critical, because he will have air supremacy and the ships will be exposed to air attacks when approaching Sevastopol or when stationed in the bays."* (KTB, A. S.M.R 2563, c. 36).

The special preparations for the evacuation from Crimea, as reported by A.S.M. to the Superior Naval Command south and to the War Navy Command, showed that upon receipt of the evacuation order, all the floating means available to the axis in Romanian ports were organized in several convoys totaling a capacity of 18,000 men and that were to arrive at Sevastopol on the evening of 11 May (KTB A.S.M., R 2563, c. 50).

Although at this stage, which bore the name *"Operation 60.000"* for the Romanian side, a good part of the transport organization was delegated to the Maritime Naval Force, the A.S.M. still held the supreme authority in naval matters. In this regard, the directives for the first convoys, which were issued on May 9, were also preserved in the following days and defined the parameters in which the transport missions were to be carried out. Taking into account the desperate situation and the imperative to recover the troops as quickly as possible, it was decided to create as large convoys as possible for anti-aircraft protection without sacrificing as much speed if possible. The old considerations regarding the allocation of sufficient escorts were now no longer applicable. The bypass road to the south was also abandoned, preferring the direct route (KTB A.S.M., R. 2563, c. 51).

At the level of the land and marine commands, tensions reached new dimensions during this period. In the foreground was Schorner, naturally worried about getting his forces back from Crimea. He was outraged by Allmendinger's reports and in a message to the A.S.M. he remarked the lack of involvement of the Romanian ships. The phrase is important because Romanian sources correctly point out

that Brinkmann and Schulz were able very quickly to debunk the allegations. But it is equally relevant that, along with Allmendinger and the leadership of the 17th Army, the matter was raised by Schulz himself on 10 May in a radiogram to Brinkmann. Seeko Krim demanded the use of all available forces in the Black Sea, *“including Romanian destroyers”*.

It is perfectly true that throughout the German-Romanian cooperation in the Black Sea, the Maritime Naval Force sought through various methods to protect these precious resources, but the accusation was tendentious. The Army sought to show through it that the Navy, especially the Romanian one, was not willing to commit all the forces, thus forcing the soldiers to stay at Chersones longer than would have been necessary. Brinkmann and then Schulz denied the accusations and showed that all the Romanian ships, going up to the destroyers, had already been used in transport missions. Commander A.S.M. it even reported that the very good partnership relationship with Admiral Macellariu ensured a superior level of understanding, and the maritime naval force engaged all *“available units up to all limits, for the success of our joint mission. There were no difficulties”*. (KTB A.S.M., R 2563, c. 50).

The day of 10 May began with the news that *“Teja”* and *“Totila”* had been attacked by Soviet aircraft after they had been evacuated. *“Totila”*, escorted by three *“R-Boot”* was attacked around 09:30 by Soviet aircraft and sunk quickly without a chance of a rescue intervention at 10:30. Of the 5,000 on board 2,000 were Romanians. There were no reports of rescue or even attempted rescue of people on the ship (KTB A.S.M., R 2563, c. 60).

“Teja” was attacked several times by enemy aviation. First at 07: 10 she suffered a fire as a result of shelling. Then at 11: 25 she narrowly escaped further attacks and was able to get men on board, nearly 5,000 (German sources mention 4,700). On the way back to Constanta, the ship was hit by aerial bombs at 12:32, the engine room being destroyed. *“Teja”* sank at 15:00, 55 miles SW of Chersones. The *“R-boats”* recovered around 400, another 130 by torpedo boats and an unknown number by the ship *“Romania”* (KTB A.S.M., R 2563, c. 60).

The loss of the two ships represented the biggest disaster of the entire evacuation mission that began in April. More than 8,000 Axis soldiers lost their lives in this attack (Forczyk, 2014, p. 290). For the A.S.M., which had accepted that losses were inevitable, the fact that the two ships nevertheless managed to approach the embarkation points as to load the thousands of evacuees, showed however that the reports of the ship commanders were exaggerated, at least for the conditions of 8-10 May.

By the afternoon the convoys “Artist”, “Thrush” and “Prophet” also suffered air attacks, fortunately with no hits on the ships (KTB A.S.M., R 2563, c. 60). The situation took a negative turn on the night of 11/12 May and during the morning, when enemy bombing planes sank the improvised minesweeper “Romania” (3,152 TRB) and the freighter “Danubius” (1,489 TRB). The German freighter “Helga” was badly damaged and put ashore. The escort tried to retaliate, mostly with the 40 mm “Bofors” guns of the destroyer “King Ferdinand”, but the ship was also repeatedly attacked by aircraft. A bomb killed 11 crew members, and then the intervention of Soviet artillery made staying in the area impossible. The conclusion was obvious: Axis ships could not linger too long in Crimean waters during the day (Forczyk, 2014, p. 290).

“Romania”, which was the main ship in the convoy “Ovidiu”, had recovered a large number of shipwrecked from a sunken German “M.F.P.”. As in the case of “Danubius”, the ship carried ammunition for the defenders of the bridgehead (Koslinski, Stănescu, 1997, p. 257). Brinkmann notes that all Constanta-Sevastopol convoys were leaving partially loaded with munitions. Once in Crimea, the assumption that they were not fully unloaded is plausible. The boat commanders and officers had orders to speed up the men’s embarkation and resend the ships back to the West. At least some of the successes of Soviet air missions can also be explained by the fact that the attacked ships had ammunition on board (KTB A.S.M., R 2563, c. 61). The reason was the insistence of the Army Group South Ukraine, which wanted the forces in the bridgehead to continue to be supplied.

The reaction of the command of the 17th Army, transmitted further high up by Schorner, is equally explainable. New allegations were made, showing that the order for ships to make the journey to Chersones had not been complied with regardless of the weather conditions. The “Thrush” convoy turned back due to the weather, then continued on its way, causing delays at the craft points. “Patria” loaded only 3,000 men instead of 9,000, the estimated maximum capacity, with Schörner fuming that the crews showed cowardice, preferring to leave with partially occupied ships rather than wait for full loading under enemy fire (KTB A.S.M., R 2563, c. 62).

This is the famous message mentioned by the Romanian sources, in which it is said that there were 35,000 Axis troops at Chersones (Koslinski, Stănescu, 1997, p. 258). The statement was part of a brief presentation of the situation on the ground and was meant to emphasize the importance of the transports for the rescue of the military forces there, as well as that of the munitions that the army insisted on requesting at any opportunity (KTB A.S.M., R 2563, c. 63). A.S.M. countered all these accusations coming from the land troops, pointing out that at the time

of issuing the code name *“Wildkatze”*, on May 8, a group of ships with an evacuation capacity of 20,000 people was immediately dispatched to Sevastopol. With Hitler’s approval for the evacuation of the bridgehead, other ships with a capacity of 35,000 men were added, raising the total in the period of May 8-9 (arrival on the 10th at the latest) to 55,000 men. A.S.M. showed that it did not rebate any ships, even using those with reduced mobility and those not completely repaired, etc. Naturally, there were also factors that limited the effectiveness of the measures, as was the case with weather conditions and the loss of extremely important craft points. The abandonment of Sevastopol, although planned, occurred faster and with greater consequences than anticipated for the German and Romanian forces. Brinkmann also stressed that both the German Navy in the Black Sea and the Romanian Royal Navy acted with conviction and at the limit of their possibilities, *“to carry out their tasks at sea and on land, with all efficiency and all the spirit of sacrifice”* (KTB A.S.M., R 2563, c. 63).

These explanations did not alleviate the state of strain that reigned at the higher land and naval commands. Brinkmann had to admit checks in the case of the convoy *“Patria”*. The fact that *“Teja”* and *“Totila”* had about 10,000 on board people indicated that it was not cowardice. On the contrary, the commanders and boat officers did their job very well, since in such a short time the loading of the ships was successful. The whole evening of 10 May saw feverish activity relating the General Staff of the Army to the Navy command and the Superior Naval Command South, requesting reports on the evacuation. Brinkmann notes that, perhaps under the influence of the 17th Army Command, the Naval Command in Crimea led by Schulz had adopted the pessimistic tone. Radio channels were flooded with a cascade of messages that had the effect of effectively blocking communications with German and Romanian ships, often provided only with a radiotelegrapher. Inconsistencies inevitably occurred and some ships actually had to blindly find their embarkation points. Soviet artillery and the danger of air attacks limited the action of the guidance ships, which were no longer able to guide the transporters to the Kasancha and Kamishevaya baths, the main embarkation points. The situation from hour to hour was constantly changing and these numerous messages added to the existing chaos (Koslinski, Stănescu, p. 257).

The arguments used by Brinkmann were correct. The schedule established with the 17th Army for the operation *“Wildkatze”* was not respected. The reality on the ground did not match the assumptions of the Army General Staff, whose resistance proved weaker against the Soviet onslaught. In these circumstances, as Brinkmann noted, *“all the A.S.M. can do is send as many ships as possible and as quickly*

as possible, regardless of the weather conditions and the actions of the enemy” (KTB A.S.M., R 2563, c. 64). His conclusion was that the naval forces could not anticipate the conduct of battles on land, and the army now sought to blame someone for its conspicuous failure.

After the end of the evacuation mission, which had obvious deficiencies in the organization and especially in the implementation, the disputes between the ground troops and the German Navy (involving the Romanian Navy) continued. Even on May 13, when the last survivors were being recovered in terrible conditions off the coast of Chersones, Allmendinger sent his conclusions about cooperation with the Navy during the mission to withdraw from the bridgehead. From the very beginning, he pointed out that from the point of view of the leadership of the 17th Army, the evacuation was affected by *“the lack of Organization of the Navy, which had profound effects”* (AOK 17, KTB no. 10, 157, f. 177). The first of his assessments, concerning the organization of the links between the army and the Crimean Naval Command, is easy to verify, and indeed the planning of the evacuation, from the number of ships involved, the wharves allocated, to the establishment of the units to be brought to certain wharves, was the result of joint work. Further, however, he overestimated the battlefield performance of the units under his command: *“The retreat from the Chersones position, the arrival to the embarkation points, the organization of Army communications and rearguard lines of resistance in the area of the craft points were made under strong pressure and under enemy fire, but according to plan.”* (AOK 17, KTB no. 10, 157, f. 177).

It is easy to understand why he did so: it was an attempt to counter the accusations of the Navy, which claimed that the established plan was not followed and that the evacuation began earlier than agreed because the resistance of the army was too weak. The effects were seen on 9-13 May, when the hastily created, convoys were desperately led to the embarkation points where disorganized troops were huddled. Here, in fact, was the key to the partial failure of the evacuation of the second stage, the tragedy unfolding between the front line and the ships offshore. In this space discipline and organization often disappeared entirely, and the two major units involved, the 17th Army and the A.S.M. each tried to pin the blame on each other.

Further on however Allmendinger’s accusations become more concrete, referring to the disorganization of convoys, whose commanders did not know for sure which embarkation points to reach. It is also true that a significant number of ships returned to Constanta without having the maximum number of soldiers on board, although in most cases partial loadings were preferred to hasten

the departure back due to the threat of Soviet air attacks. Allmendinger concluded that: *“To clarify the situation and detail it, a large-scale hearing will be required. It is unfortunate that, due to the reported deficiencies, a good part of the defense troops that were still fighting at Chersones, were no longer evacuated. It is undoubted that their evacuation would have been in difficult conditions, but it could have been done according to the transport schedule and on a much larger scale than was achieved.”* (AOK 17, KTB no. 10, 157, f. 178).

On the same day, the Journal of Combat Actions of the A.S.M. included several points that explained in good part these shortcomings:

“In addition to them, another 6,000 soldiers were boat and not recovered, being on ships lost in the attacks. In any case, the sending of ships lasted until 10 May. The supply of the fortress exceeded the requested average. Despite the use of all available ships, troops remained to be carried out, strictly due to factors outside the control of the Navy, such as:

- 1) insufficient time to prepare the floating material (at least 36 hours, minimum required for the bypass route chosen by A.S.M.);*
- 2) hasty withdrawal of the Army because the enemy has penetrated the line of contact. The studies and plans prepared by the 17th Army provided for an orderly withdrawal, in 3 stages, each of which further shortened the line of contact and with evacuations at each step. In fact, however, the Army was forced by the enemy to immediately retreat to the Chersones (Chersones position), leaving behind the intermediate positions, so only 3 days were available for evacuation;*
- 3) total air superiority of the enemy during the 3 days;*
- 4) powerful artillery fire on all embarkation points, improvised positions; the batteries could not be deafened by our forces or our own aviation;*
- 5) bad weather conditions on May 10, so the transports and “M.F.P.” units were delayed and did not arrive on time at times (especially at night);*
- 6) boat problems were accentuated by artificial fog (fumigants), smoke etc., which made it difficult to find loading points even for commanders who were familiar with the area.”* (KTB A.S.M., R 2563, c. 86).

It is clear that the clarifications brought by the A.S.M., also assumed by the Navy Command in Berlin, were not able to block the efforts of the 17th Army leadership, which now even demanded that the Navy officers be court-martialed. That's because on May 21 Allmendinger formally requested the commander of Army Group South Ukraine to represent the interests of the 17th Army and initiate court-martial investigation proceedings, pointing out that the decoration of admirals

Brinkmann and Schulz with the Knight's Cross of the Iron Cross was an offense for the sacrifice of soldiers who could not be evacuated by the two sailors themselves *"organizers of the evacuation of Crimean fighters"* (AOK 17, KTB no. 10, 157, f. 71).

Other arguments in favor of the idea that the naval units did not do their duty to their comrades in the land troops were brought later, as was the case with the criticism of the inability of the A.S.M. to evacuate the wounded early before the start of the large-scale evacuation operation. On the other hand, the claim that due to transport delays the army was deprived of the necessary reinforcements (two infantry divisions) was obviously tendentious. The same is the case for other charges; basically, Allmendinger was blaming the A.S.M. leadership that it misreported on 7 May of having sufficient transport space not only for the emergency withdrawal of the first wave (20,000 troops), but also of the rest of the forces at Chersones no later than 9 May. Here Allmendinger launched himself into supposition, because Brinkmann had in fact reported that he could secure the evacuation of 20,000 troops and, *"if the ships are used at full capacity"*, perhaps even 25,000 (KTB A.S.M., R 2563, c. 43).

The other points Allmendinger touched upon in his report to the Berlin superiors carry more weight. Much of the floating material was sent on May 10, too late according to Army leadership. What is omitted however is that Hitler only approved the evacuation of the remnants of the 17th Army on 9 May. The first convoys left in fact on the 9th, but other factors made it difficult to travel, as was the case with the need to group the ships into larger formations, in order to provide anti-aircraft protection at least partially (KTB A.S.M., R 2563, c. 51). Brinkmann also noted that an essential condition for the success of the mission was that the Army would hold out until 12 May, in order to keep the Kasancha and Kamishevaiy bays, which proved impossible.

Allmendinger's report included numerous testimonies from commanders and other officers and non-commissioned officers in army units, which essentially documented the chaos and lack of coordination that characterized the last two days of the evacuation. The answer to all the accusations can be considered Brinkmann's report, which we reproduce here: *"On the consultations between the commander and the head of the Superior Naval Command south, I report that Colonel General Schorner's very violent accusations against the Navy relate to her inability to transport troops from the Crimea. He requested further information on naval actions, as he was due to send the final report to the Fuhrer by 13:00. The conversation with Colonel General Schorner was abruptly interrupted when I showed all the difficulties, provoked by weather conditions, the actions of the enemy*

and that the final figures are not available. I confirm that I have been ordered not to discuss naval operations and other similar information with the military. Moreover, I report that General Hartmann publicly approached the head of the Crimean Naval Command (in the Carlton Hotel) and criticized the Navy.

According to the general's statements, I suspect that the following allegations have been made against the Navy:

a) despite the close cooperation between Seeko Krim and the 17th Army, regarding the craft points and troops assigned to each, the ships did not arrive in time to retrieve them.

Answer: see the paragraph corresponding to the night of May 12. There is plenty of craft space at Chersones. Due to smoke camouflage and fog, identification of embarkation points was done by Seeko personally, sailing on torpedo boats, which guided the ships waiting at Chersones.

b) ships were not assigned embarkation points at times.

Answer: as much as possible due to significant crowding, Seeko informed the ships of the wharves and wharves in a timely manner. It should be pointed out that more than 60 boats arrived simultaneously and had to be routed by radio.

c) a few ships were too far from the coast to embark.

Response:

The allegations probably relate to the case of "Totila" and "Teja", which has already been clarified. Both ships had a total of 8,700, loaded to the limit, damaged by bombs shortly after the craft and sank.

d) Seeko left the command post at Maxim Gorki 2 before the completion of the craft.

Response:

Seeko left the command post on the last night of the evacuation at 21:00. Command of the troops there was impossible because ties were severed. He sailed on a torpedo boat and steered the arriving ships and the "M.F.P.s" to the loading points. He remained at Chersones until sunrise. Other boats were no longer possible because of the enemy. Seeko Krim's decisions were appropriate.

e) the transport ships were stopped on the night of 12 May at 32 degrees east and were no longer used.

Response:

After receiving the message that the craft should be stopped after the night of 12 May, the ships were still en route to Chersones and stationed at 32 degrees east, with orders to intervene if necessary to: a) provide support in case the transport ships suffered damage on 13 May; b) provide embarkation if despite the information

the embarkation points could be used. The ships moved immediately although they could not reach them until sunrise. There was sufficient tonnage for the forces that were identified at Chersones.” (KTB A.S.M., R 2563, cc. 86-91).

In the end the complaints of the leadership of the 17th Army were without the expected result. Admirals Brinkmann and Schulz retained the decorations and the explanations given were convincing. Indeed, it should be pointed out that the loss of the several thousand soldiers who could not be evacuated was the result of a complex of factors that were difficult to predict, the effects of which proved even harder to avoid. From the temporary halt of the evacuation after the first phase, to the overly optimistic assessments and plans about the evacuation “*in one move*”, to the loss of the defensive positions at Sevastopol, all inevitably led to greater losses than had been initially accepted. In the end, the situation on the ground, the total mastery of the air by the enemy and the inherent confusion could not but have negative effects on the evacuation mission in the Crimea.

BIBLIOGRAPHY:

1. A.M.N.R., Headquarters Naval Maritime Forces (C.F.N.M.), file 33/1943.
2. A.M.N.R., fund Undersecretary of State of the Navy (S.S.M.), file 26, file 3055.
3. AOK 17, Anlage 6 zum KTB no. 10, 1.4-30.6.44, Findbuch 12473, Akte 157.
4. AOK 17, Sonderband zum KTB no. 10, Vortrag OB Beim Fuhrer, Findbuch 12473, Akte 150.
5. Buttar, P. (2020). *The Reckoning. The Defeat of the Army Group South 1944*, New York, Osprey Publishing.
6. Forckzyk, R. (2014). *Where the Iron Crosses Grow – the Crimea 1941-1944*. Oxford, Osprey Publishing.
7. Koslinski, N., Stănescu, R. (1997). *Marina Română în Al Doilea Război Mondial (1939-1945). Volumul II (1942-1944)*. București: Editura Făt-Frumos.
8. KTB Admiral Schwarzes Meer, 1 May-15 May 1944, National Archives Microfilm Publication, T-1022, R 2563.
9. KTB Admiral Schwarzes Meer, 16 Apr.-30 Apr. 1944, National Archives Microfilm Publication, T-1022, R 2592.
10. Schonherr, K. (2007). “*The Alliance of Army Group A through the Crimea to Romania*”, in Karl-Heinz Frieser, *Germany and the Second World War, Vol. VIII, The Eastern Front 1943-1944: the War in the East and on the Neighboring Fronts*. Oxford: Clarendon Press.

RADIOGRAPHY OF MILITARY UNITS FROM BAIA MARE GARRISON FROM 1990 TO 2005

Chaplain Gavril Vasile BĂBAN

Military Church „Sf. Mare Mucenic Gheorghe – Purtătorul de Biruință”, Baia Mare

DOI: 10.55535/RMT.2025.3.42

Military life is marked by vocation, dedication, loyalty and professionalism. The Baia Mare Garrison is one of the places where such soldiers and representatives of the entire corps of personnel categories in the Romanian army can still be found and who marked the period of 1990-2005. In the context of the last years, 2020-2025, marked by challenges to peace, especially in the Black Sea Emergent Zone, the need to affirm the principle and reality of training is reaffirmed, the ability to operate with professionalism the entire package of capabilities specific to each military unit for men to restore peace, by arming the entire professional of the personnel we have. This scientific approach presents the military structures in the Baia Mare garrison through a documentary analysis.

Keywords: military units; Baia Mare; readiness; training; military personnel;

POLITICAL AND HISTORICAL CONSIDERATIONS SPECIFIC TO THE 20TH CENTURY

On 14 May 1955, a new political-military bloc was established, the Warsaw Pact organization. The signatories of this treaty were the countries under the direct influence of the Soviet Union, forming the European communist bloc: Poland, Hungary, Czechoslovakia, the GDR, Bulgaria, Albania, and Romania. Although the *"Treaty of Friendship, Cooperation and Mutual Assistance"*, known historically as the *"Warsaw Pact"*, had been conceived as a strictly defensive security organism, the alliance was created as a response to the emergence of the Western military alliance NATO in 1949 and to the inclusion of West Germany in NATO in 1955.

Between 1962 and 1968, a series of international events led to the weakening of the Pact and to Romania's increasingly pronounced *"dissent"* within it. Among the most significant events were: 1962 – Albania's formal withdrawal from the Warsaw Pact (its official withdrawal occurred in 1968); the coalition of China, Yugoslavia, Hungary, and Albania during the Sino-Soviet conflict; Romania's firm reaction in 1965 when it practically issued its *"declaration of independence"*, demanding the cancellation of Albania's exclusion from the treaty; the severe crisis caused by the placement of Soviet nuclear missiles in Cuba (1962) without the knowledge or consent of the Pact members, followed by Romania's formal distancing from this action before U.S. authorities (Corneliu Mănescu, as Minister of Foreign Affairs, drafted a letter delivered to U.S. Secretary of State Dean Rusk, expressing Romania's position); the USSR's attempt to expand the Pact in 1963 by including the Mongolian People's Republic as a full member; the attempts to reject military integration processes within the organization and the breach of the Treaty's fundamental principles; attempts to subordinate the Romanian and Bulgarian naval fleets to the Black Sea Fleet Command; Romania's refusal to allow Soviet troops to transit its territory or to concentrate Romanian troops in Bulgaria for joint exercises in 1964; the proposals advanced in 1966 by Romania regarding the de-Sovietization of the Pact's leadership; Romania's refusal to sign the *"Moscow Declaration"* of 9 June 1967 concerning the Arab-Israeli conflict known as the *"Six-Day War"*, as Ceaușescu opposed the Soviet position condemning Israeli aggression and promising increased support for Arab states.

These events, among many others, strengthened Romania's reformist position within the Pact. They also contributed to the drafting of the well-known document *"On the Action Program of the Czechoslovak People's Army"*, also known as the "Klement Gottwald Academy Memorandum," initiated by the rector of the Military Academy in Prague and another senior officer. The memorandum, supported by Poland, Hungary, and Romania, along with the civil actions of the group *"Charter 77"*, constituted some of the key elements that triggered the Warsaw Pact's military intervention in Czechoslovakia in August 1968. The invasion took place without convening – even formally – the Political Consultative Committee, which would have allowed consultation with all member states.

It is telling that Romania was neither asked to participate in nor informed about the preparation of the intervention – Soviet leaders being fully aware of Romania's stance within the Pact.

The period following the Czechoslovak crisis marked the beginning of the development of Romania's national military doctrine, with a specific content aligned with the political-military context within the Warsaw Pact. Military historians argue that an immediate intervention in Romania following that in Czechoslovakia would have caused major international complications, amplified by global public opinion and detrimental to the Soviet Union's image. Moreover, Romania's territory was much larger, no Soviet troops were stationed on its soil, and no Pact exercises were being held there, making surprise aggression unlikely. Soviet intelligence networks had been uncovered since 1962, and their activity was monitored and counteracted by Romanian counterintelligence.

Given the limited access to Moscow's archives, evaluating the Kremlin's intentions toward Romania during the Czechoslovak crisis remains extremely difficult, if not impossible (Betea, 2009, p. 38).

In terms of geopolitical and geostrategic positioning within the Warsaw Pact, the Romanian Army was assigned two strategic defensive directions: the Greek-Turkish and the North-Italian. Consequently, Romanian military units were primarily deployed between the Carpathians and the Danube, in central and western Romania.

The events of the summer of 1968 provided Romania with guidance in defining its future political and military position within the Pact and toward the Soviet Union. As required, the military doctrine had to be strictly defensive, distinctly different from the Soviet one. Under the circumstances, national defense could be ensured only by Romania's own forces.

On 11 September 1968, during a meeting of Romania's political-military leadership, important decisions were adopted to prevent a possible invasion

by Warsaw Pact forces. Measures for improving the distribution and structure of Romania's armed forces were approved.

As a result, Romanian military authorities began defining a unique defense doctrine without precedent within the Pact, which – combined with Romania's foreign and military policy – emptied Romania's membership of the Pact of its military substance, even though Romania never formally requested withdrawal. Substantial changes were made to the structure, equipment, endowment, and training of the national defense system. Romania's military ties with the Pact gradually diminished. Nonetheless, the political posture toward the Soviet Union, defined by *"intransigence – compromise"*, did not diminish the Kremlin's vigilance regarding a potential Romanian *"defection"*.

A relevant account is provided by General Anatoly I. Gribkov, former Chief of Staff of the Pact's Unified Armed Forces (1976-1989), who stated: *"Gradually and in secret, troop deployment was revised. The divisions with the highest combat capability were deployed near the Soviet border toward the so-called 'Focșani Gate' and near the border with Bulgaria. Later, the Hungarian direction – Transylvania's disputed territory – was reinforced."* (Gribkov, 1998).

The international developments and the armed intervention in Czechoslovakia beginning on the evening of 20 August 1968 triggered strong reactions from the Romanian government and corresponding military measures. The Minister of the Armed Forces, General Ion Gheorghe, ordered: *"If we are attacked, we will retaliate."* (Documentary Report No. 248/23.07.1998, UNCMRR, p. 3), an order communicated down to unit commanders.

"At the level of the 3rd Army, a defense and intervention plan was drafted for the main northern and northwestern directions, while reservists were mobilized between 21-24 August 1968, nearly doubling combat capacity. In a matter of days, patriotic guard battalions and companies were formed and armed. Each county established the command staff for the patriotic guards."

Furthermore, due to the weaker military presence in the Transylvanian lowlands and hills, the Council of Ministers' Decision No. 1991/13.09.1968 established the creation of the 81st Mechanized Division on 1 October 1968, subordinated to the 3rd Army, with its command in Dej. It included: Regiment 221 Mechanized in Bistrița, Regiment 223 Mechanized in Dej, Regiment 4 Mechanized in Zalău, Regiment 230 Tanks in Baia Mare, Regiment 612 Antitank Artillery in Baia Mare, Regiment 313 Artillery in Șimleu Silvaniei, Battalion 422 Engineers in Satu Mare, Division 55 Anti-Aircraft Artillery in Dej, Battalion 424 Signals in Dej, Battalion 87 Engineers in Dej, Company 302 Supply and Transport in Șimleu Silvaniei, Platoon 283 NBC Defense

in Dej, Platoon 368 Anti-Aircraft Command in Dej, Company 394 Traffic Control in Dej, Workshop 925 Artillery in Șimleu Silvaniei, Workshop 345 Tank and Auto Repair in Baia Mare.” (Armata a 4-a “Transilvania”, vol. IV, 1945-1999, p. 156).

Through these historical and political-military considerations, we place within the events of the late 20th century the moment and significance of establishing in Baia Mare, in autumn 1968, alongside other units in northwestern Romania, the 612 Antitank Artillery Division, the 230 Tank Regiment, and the 345 Tank and Auto Repair Workshop, as well as other military units in Maramureș County.

MILITARY UNITS IN MARAMUREȘ¹

Before the Great Union of 1918, more than 10,000 men from Maramureș fought in the Austro-Hungarian Army, most of them enlisted in Infantry Regiments 85, 5, and 12, stationed in the Sighet garrison. They fought on the fronts in Galicia, Serbia, Ukraine, and Italy, in the major battles of Lemberg, Doberdo, Manilowa, and Piave. Throughout the entire conflict, the Austro-Hungarian Army included three generals (Ioan Boeriu, Gheorghe Domășneanu, Dănilă Papp), 15 colonels, and 12 lieutenant colonels of Romanian origin.

Through Ministerial Decision No. 40 of 26 January 1919, the Territorial Command 6 Cluj – named in wartime the 20th Infantry Division – was established in Transylvania. Subordinated to it were several newly established military units, including those deployed in Maramureș County [Col. (r.) Ioan Bota, President of the Maramureș County Branch of the National Association “*Cultul Eroilor Regina Maria*”, *Prezențe ostășești pe meleaguri maramureșene* – unpublished manuscript).

The 88th Infantry Regiment/Regimentul 88 Infanterie Sighet

Established on 6 June 1919, based on Battalion 3 of Regimentul 81 Infanterie Dej, deployed in the Sighet garrison, headquartered in the barracks on Tokoly Street (today, Dragoș Vodă Street). Its mission was to participate in the defense of the newly established borders of the Romanian state. The regiment was relocated to Careii Mari in 1921 and disbanded on 26 October 1938.

The 52nd Infantry Brigade/Brigada 52 Infanterie Sighetu-Marmației

Established on 16 August 1919 under Ministerial Decision and War Minister Order No. 2593 of 26 January 1919. It consisted of Regimentul 103 Infanterie (Satu Mare) and Regimentul 104 Infanterie, the latter being on the Tisa front at that time. The Brigade operated in Sighet until 1923, when its personnel were transferred to Regimentul 88 Infanterie, headquartered in Careii Mari.

¹ Col. (r.) Ioan Bota, president of the Maramureș County Branch of the National Heroes Cult Association “*Regina Maria*”.

The 103/104th Infantry Regiment/Regimentul 103/104 Infanterie Sighet

Established based on General Staff Order No. 5170 of 6 September 1920. Beginning 1 October 1920, it unified with Regimentul 103 Infanterie. It had its Headquarters and 1st Battalion in Sighetu Marmăției, and the 2nd Battalion in Satu Mare. It remained in Sighet until July 1923, when it was disbanded, with its personnel absorbed into Regimentul 88 Infanterie Careii Mari.

5 Mountain Cannons Division/Divizionul 5 Tunuri Munte

Established through Royal Decree No. 1674 of 12 April 1923, using personnel and equipment from Divizionul 2 Artilerie Munte (Codlea, Brașov County). Relocated to Sighetu-Marmăției, it became subordinate to Divizia 2 Vânători de Munte and was stationed in the Dragoș Barracks. Its structure included: commander, deputy commander, mobilization officer, adjutant, cashier, clothing NCO, and multiple batteries and support sections.

The division took part in numerous exercises, including the 1934 Royal Maneuvers in Câmpeni and the major 1936 maneuvers in the Sighet–Vadu Izei–Berbești–Călinești–Budești area. It left Sighet after the territorial losses of 1940 and settled in Aiud by 5 September 1940.

The 5th Mountain Hunters Group/Grupul 5 Vânători de Munte

Established in 1925 in Sighetu-Marmăției, comprising Battalions 9 and 10, under Brigada 2 V.M. In 1937, Colonel Leonard Mociulschi became commander. The group established a permanent ski training center at Lutoasa in the Maramureș Mountains, near the Vaser Valley.

Between 1939–1940, the group was deployed in defensive positions along the north-western border (Vârful Stog-Halmeu), undertaking intense fortification work and countering Hungarian infiltration attempts. The retreat ordered after the Vienna Award of 30 August 1940 deeply affected the troops, as recorded in the historical log of Battalion 8 V.M.

After WWII, a Mountain Troops Training Center was established in Borșa in January 1949, subordinated to Battalion 14 V.M., training hundreds of officers, NCOs, and soldiers until its disbandment later that year.

The 27th Mountain Battalion/Batalionul 27 Vânători de Munte “Bogdan Vodă”

Following the approval on 9 November 1973 of the plan for reorganizing and equipping the Romanian Army (1976–1980), Brigada 1 Vânători de Munte was established on 1 January 1977, headquartered in Bistrița. Batalionul 27 Vânători de Munte was created in Borșa, in a former military medical facility transferred in 1953. The battalion received its Battle Flag in summer 1978.

Between 1978–1989, the battalion achieved notable results in combat training, alpine and ski instruction, and mountain warfare skills. Between 1990-2005, it continued to perform successfully, with an increasingly mature and stable cadre. In 1992, it was awarded the honorific title “*BOGDAN VODĂ*”. On 7 July 1997, marking its 20th anniversary, it received a new Battle Flag through Presidential Decree No. 301/1997.

The 9 Radiolocation Company/Compania 9 Radiolocație Vișeu de Sus

A subunit subordinated to the Romanian Air Force Staff, tasked with aerial surveillance of the northern region of the country, operating radars from Vârful lui Dan.

THE BAIJA MARE GARRISON

The 7th Border Guard Regiment/Regimentul 7 Grăniceri Baia Mare

After the Great Union of 1918, one of the Romanian state's first measures was establishing major border guard units to protect the north-western frontier. Through Royal Decree No. 1559 of 7 May 1931, Regimentul 7 Grăniceri was established in Baia Mare, with its sectors secured by battalions stationed in Sighet and Oradea, under Brigada 4 Grăniceri. The regiment guarded 452.594 km of borders (with Poland, Czechoslovakia, and Hungary).

It was organized with its command structure and several specialized services, including mobilization, security and intelligence, firing training, logistics, and depot companies. The first commander was Lt. Col. Ionescu Vasile. The regiment established its headquarters on Episcopul Pavel Street No. 10 (today the Maramureș County Archives). Its strength was 1,900 soldiers.

In 1932, under a secret order, units of the regiment participated in maintaining public order in Baia Mare, Arad, and border sectors. On 10 May 1933, it received its Battle Flag in a ceremony in Bucharest attended by King Carol II.

Between 1935-1937, the regiment was commanded by Colonel Petrescu Gheorghe, later honored by the City of Baia Mare in 2006. In 1938, the Corps of Border Guards reorganized into Border Guard Groups, creating Grupul 7 Grăniceri Pază in Baia Mare.

After general mobilization on 27 June 1940 and the Vienna Award, Grupul 7 Grăniceri relocated to Cluj, then other garrisons. Border Guard troops returned to Maramureș on 1 January 1946, reestablishing Regimentul 7 Grăniceri Pază in Baia Mare.

Between 1949-1960, the regiment was resubordinated several times. In 1969, a commission proposed relocating border posts deeper into Romanian territory

to avoid direct Soviet observation. New posts were built mostly along the Vaser Valley.

After the regiment's disbandment, the Sighet Border Guard Battalion was subordinated to Brigada 5 Grăniceri Oradea.

The County Military Centre/Centrul Militar Județean Maramureș

After 1918, a County Military Center functioned in Sighetu Marmăției. Following the administration's withdrawal from Northern Transylvania, the structure was disbanded. After territorial reorganization in 1950, Comisariatul Regional Maramureș was created, with several subordinate district commissariats.

On 17 February 1968, under Law No. 2/1968, the Centrul Militar Județean Maramureș was established, subordinated to the First Deputy of the Minister of Armed Forces and Chief of the General Staff.

On 15 January 1990, under Order MC 3/1990, the Comandamentul Militar Județean Maramureș was established, incorporating Civil Defense and Patriot Guards Staffs and an intelligence office. The structure reverted to Centrul Militar Județean in 1994 and underwent several organizational changes until 2007.

During this period, a Soviet military commissariat and regional military prosecution office also functioned in Baia Mare until Soviet units withdrew in 1958.

The Civil Protection Inspectorate/Inspectoratul de Protecție Civilă Județean

Between 1952–1978, civil defense operated under the Local Anti-Aircraft Defense Staff, subordinated first to the Ministry of Interior and later to the Ministry of Defense. From 1978-2006 it functioned as the County Civil Protection Inspectorate.

The inspectorate responded to major floods (1970, 1993, 1995, 1998, 2000), landslides (1980, 1999), radioactive contamination following the Chernobyl accident (1986), and the technological accident at S.C. AURUL S.A.

Following the 1968 invasion of Czechoslovakia, Romania strengthened its territorial defense, established new units, and mobilized reservists. In this context, Divizia 81 Mecanizată was created, including several units stationed in Baia Mare: Regimentul 230 Tancuri, Atelierul 345 Reparații Tancuri și Auto, and Divizionul 612 Artilerie Antitanc.

The 230th Tank Regiment/Regimentul 230 Tancuri

Established in 1968, the regiment initially shared the same barracks with two other newly created units. By 1971, construction of the new barracks was completed. In 1974, work began on the new artillery barracks, completed in 1976. Around the same time, the 345 Technical Repair Section's facilities were completed.

Initially organized with two battalions, a third tank battalion was added in 1969. In 1970, the regiment moved to the new barracks, and the tank training range

and automated firing range (Arieșul de Pădure) were completed, largely through soldier labor.

On 1 November 1990, the regiment received the honorific title *“Pintea Viteazul”*.

On 1 September 1994, it transformed into Brigada 230 Infanterie Moto *“Pintea Viteazul”*, subordinating multiple battalions and artillery divisions. It was disbanded on 30 June 2003 under national army restructuring plans.

Section 345 Military Technical Repair/Secția 345 Reparații Tehnică Militară

Established in 1968, subordinated to Divizia 81 Mecanizată, structured with a command element, technical and financial offices, tank, auto, artillery, signals, and special equipment workshops, and evacuation teams. It was resubordinated to Corpul 7 Armată *“General Nicolae Șova”* (1994-2000), then Brigada 230 Infanterie Moto *“Pintea Viteazul”* (2000–2003), and disbanded on 1 April 2003.

Antitank Artillery Division 612/Divizionul 612 Artilerie Antitanc

Established on 1 October 1968, subordinated to Divizia 81 Mecanizată, and awarded its Battle Flag on 15 December 1968. In 1969, it became Regimentul 612 Artilerie Antitanc, initially organized with two divisions, later three.

It moved to its new barracks on Bulevardul Unirii on 12 February 1976. In 1979, it became subordinated to the 3rd Army (later 4th Army). In 1990, it received the honorific title *“Maramureș”*.

In 1994, it was reassigned to Corpul 7 Armată *“General Nicolae Șova”*, and on 1 September 1994 became Brigada 612 Artilerie Antitanc. In 1996, it received a new Battle Flag through Presidential Decree No. 111.

It underwent multiple reorganizations between 2002–2008, transitioning from brigade to regiment to division to battalion. In 2007, it received the honorific title *“Maramureș”*. Since 1 January 2022, under Order M-0225/2020, the unit became Batalionul 813 Infanterie *“Maramureș”*, subordinated to Brigada 81 Mecanizată *“General Grigore Bălan”*.

INSTEAD OF CONCLUSIONS

The strategic and tactical military vision aligned with Romania’s national defense doctrine generated highly capable military structures such as those presented above. Their equipment, but especially the quality of their human resources, decisively contributed to fulfilling their missions. Soldiers from Maramureș have consistently demonstrated professionalism, preparedness, and the moral qualities of the authentic Romanian serviceman – a legacy carried forward by today’s active military personnel (2025).

BIBLIOGRAPHY

1. „*Amor patriae nostra lex*”. The publication was edited on the occasion of the 50th anniversary of the establishment of the 612th “Maramureș” Anti-Tank Artillery Battalion, Baia Mare, 1 October 2018.
2. Arhiva MAPN, fond A4, dosar 2103.
3. *Armata a 4-a „Transilvania” – Istoria unei jumătăți de veac* (1999), vol. IV, 13 May 1945 – Sept. 1999. Cluj-Napoca: Editura Dacia.
4. Betea, L. (coord.), Diac, C. (2009). *21 august 1968. Apoteoza lui Ceaușescu*. București: Editura Polirom.
5. Col. (r.) Bota, I., președintele Filialei județene Maramureș a Asociației Naționale Cultul Eroilor “Regina Maria”, *Prezențe ostășești pe meleaguri maramureșene* – mss nepublicat.
6. Documentar informativ, nr. 248/23.07.1998 al UNCMRR.
7. Duțu, Al. (1979). *File de istorie*, nr. 6-7. București: Editura Militară.
8. Gribkov, A.I. (1998). *Sudba Varșavskogo Dogovor. Vospominania, dokumenti, fakti*, Russkaia Kniga. Moscowa.
9. *Legea nr. 14 din 28/12/72 privind organizarea apărării naționale a Republicii Socialiste România* (1973). București: Editura politică.
10. Opreș, P. (2016). *Desființarea și reînființarea marilor unități românești de vânători de munte (1961-1976)*, in “*Document. Buletinul Arhivelor Militare Române*”, year XIX, no. 3 (73)/2016, pp. 67-76, https://www.researchgate.net/publication/340091417_Desfiintarea_si_reinfiintarea_marilor_unitati_romanesti_de_vanatori_de_munte_1961-1976_in_Document_Buletinul_Arhivelor_Militare_Romane_an_XIX_nr_3_732016_p_67-76, retrieved on 22 May 2025.
11. Petrescu, Gh. (2007). *Cer și pământ*. Baia Mare: Editura Universității de Nord.
12. *Registrul de ordine de zi al R. 612 Artilerie Antitanc*, 1979.
13. *Registrul Istoric al Brigăzii 612 Artilerie Antitanc*.
14. *Registrul Istoric al Brigăzii 230 Tancuri*.
15. *Registrul istoric al Regimentului 230 Tancuri*.
16. *Registrul istoric al Regimentului 612 Artilerie Antitanc*.
17. Gl.bg. (r.) Urdoi, F., *Regimentul 230 Tancuri Baia Mare, oameni de oțel* – anniversary speech on the occasion of Romanian Armoured Forces Day – 1 August.
18. Mr. Vaida, S.V. (1998). Documentar Tv – “*30 de ani de traiectorii precise*”, Cluj-Napoca.

THE SOVIET INFANTRY MAN ON THE PRUT RIVER: 22 JUNE 1941 – HISTORIOGRAPHICAL PERSPECTIVE ON COMBAT TRAINING –

Sergeant Major Ioan-Dan POPOVICIU

Comandamentul Corpului Multinațional Sud-Est, Sibiu

DOI: 10.55535/RMT.2025.3.43

In the wider field of universal historiography, the predominant depictions of the Soviet infantryman tend to oscillate between two opposing archetypes. On the one hand, the Soviet soldier is depicted as a physically imposing figure – an almost mythical giant – portrayed as superior to his opponents in terms of strength, combat effectiveness, and morale, often characterized by exemplary levels of equipment and rigorous training. On the other hand, alternate narratives cast the Soviet infantryman as a primitive or savage individual originating from the Asian steppes, described as a combatant sent into battle with minimal armament and under threat of encirclement or annihilation by superior enemy forces.

Technically, the equipment, training protocols and organizational structures of the Red Army rifle units had significant similarities to those of their Romanian counterparts. Despite differing ideological and operational doctrines, basic weaponry shared comparable characteristics in terms of design, manufacturing quality, and tactical utility. These common points suggest a level of standardization and inter-army influence that has crossed ideological boundaries in the period studied.

This paper aims to explore these issues in depth by analyzing a range of primary sources, including official archive documents, military manuals, along with secondary academic papers that examine the socio-historical processes involved in transforming the average Soviet citizen into a fully equipped and trained Red Army rifleman. Through this multi-source approach, the study seeks to elucidate the socio-military mechanisms that supported the mobilization, indoctrination and professionalization of Soviet infantry during the relevant historical period.

Keywords: training; equipment; rifleman; demographic recruitment pool; Red Army;

INTRODUCTION

On March 29, 1940, Vyacheslav Molotov, People's Commissar for Foreign Affairs of the Union of Soviet Socialist Republics (USSR), made a public statement at the Supreme Soviet session, characterized by aggressive rhetoric directed against Romania. In his speech, the central point of the Soviet argument was the assertion that peaceful relations between the USSR and Romania could not be achieved until the Bessarabian issue was resolved. This position was accompanied by diplomatic and media pressure, exerted both through official channels and through interventions in the framework of diplomatic relations between the Romanian and Soviet authorities. All these attempts ended once France was defeated by Germany, in June 1940. On June 21, 1940, the Kiev and Odessa military regions received an official order, which stated that *"Bessarabia must be wrested from the robber hands of boyar Romania."* (Constantiniu, 2017, p. 361). This was achieved by July 4, 1940, when the Romanian troops and administration withdrew to the right bank of the Prut, on the new border imposed by the USSR. These territorial gains and temporary successes were short-lived, as, in June 1941, the Romanian armed forces crossed the Prut again, to liberate the territory occupied by an enemy they *"did not value too much."* (A.M.R.P., 1940, f. 25), thus reflecting an attitude of rejection and antagonism towards the Soviet aggression on the national territory. The image of the Soviet adversary within Romanian military historiography is characterized by a certain ambiguity and lack of clarity, as a result of the fact that, for almost four decades, this field was subject to significant influence from the communist regime, which oriented and controlled the interpretation of historical events. Consequently, the issues related to the detailed knowledge of the enemy located west of the Prut River were often omitted or treated superficially, being passed over in silence in the official discourse. Only with the collapse of the communist regime in 1989, and, implicitly, with the liberalization of access to archival sources and documents, historians had the opportunity to study Operation Barbarossa in depth and critically, and, at the same time, the characteristics and human component of the Soviet army of that period. In what follows, I intend to offer my own perspective on the Soviet soldier facing the Romanian army in June 1941, attempting to present relevant

aspects of the equipment, organization, and structure of the Soviet infantry troops, as well as their recruitment and training methods. I believe that this approach, based on the analysis of historical archival documents and secondary sources that address the way in which a simple Soviet citizen became a Red Army infantryman, can contribute to a deeper understanding of the enemy's military profile and human resources, in the complex context of the summer 1941 campaign.

RECRUITMENT AND TRAINING BASE

The Workers' and Peasants' Red Army, as the Soviet Red Army was called (1918-1946), was, in June 1941, the largest army in the world. A large part of the Red Army's divisions were located on the borders with Germany and Romania. Although numerically it had the largest mechanized force in the world, the Red Army was still a force composed predominantly of infantrymen (Zologa, 1984, p. 14)¹.

From a legislative point of view, the Soviet Constitution of 1936, in Article 133, stipulated that *"the defense of the country is a sacred duty of every Soviet citizen"* (Soviet Constitution, 1936). To implement this provision, the law on universal military service was adopted, which imposed on all men, regardless of race, nationality, religion, level of education, social status or ethnic origin, the obligation to participate in the defense of the country². The only citizens who could avoid compulsory military service were those with physical deformities or mental problems. Consequently, in the event of war, all physically and mentally fit Soviet citizens were to participate in the war effort in one way or another. According to the 1939 census, the Soviet Union had a population of 170,000,000, mostly rural. This population was not uniform, being composed of 60% Russians, 16.5% Ukrainians and 3% Belarusians, the rest of the population being composed of Uzbeks, Tatars, Georgians, Azerbaijanis and Armenians. Of these, 37,000,000 were citizens aged between 20 and 39 (Schechter, 2015, p. 7). These 37,000,000 Soviets could be called up at any time for military service.

In the heavily regimented Soviet society, military training began in primary school and continued until the end of schooling. This general military training consisted of physical exercises, political indoctrination, and pre-military summer

¹ According to some sources, the Red Army had 28,000 armored vehicles, many of which were tanks that were no longer adapted to the new conditions on the battlefield. For more details, see Steven J. Zologa, *The Red Army of the Great Patriotic War 1941-45*. Oxford: Osprey Publishing, 1984, p. 14

² For more details, see <https://www.prlib.ru/en/history/619624>, retrieved on 30 August 2025.

camps. At the end of the 10th grade, for example, students received a “*certificate of maturity*”, which designated them as fit for military service. It is worth noting that in rural areas, training was more theoretical, due to the lack of materials for practical training exercises with weapons and other defensive means, but also due to the lack of adequate spaces for these training sessions.

The quality of theoretical education was also questionable, as it was provided either by a reserve officer or by a non-commissioned officer without specialized training. The situation was different, however, in cities that had a garrison from which the authorities could borrow both materials and experienced personnel to conduct training activities (Rottman, 2007, p. 10).

The district military commissariat was directly responsible for sending out the enlistment orders. These orders specified a date and a place where prospective soldiers were to report for registration. Most often, the assembly place was the local school. Upon reporting, recruits underwent a rudimentary medical examination to determine whether they were fit for military service. From there, accepted recruits were transported by train to district mobilization centers. At these centers, recruits were registered, underwent another medical examination, were dewormed, and received standard military equipment. This equipment consisted of a set of uniform, two sets of underwear, a cap, boots, a belt, and puttees (Ib., p. 8). Once examined and equipped, recruits were subjected to a harsh disciplinary regime.

The young recruit was also taught how to march in cadence, which he had to perform during field exercises and maneuvers. The training program began daily at 05:00 and lasted between 10 and 12 hours, depending on the training theme of the day. During this interval, there were short breaks and a one-hour lunch break. During tactical exercises, which involved the deployment of troops in the field, live ammunition was used to familiarize with the danger. As for patriotic education, there were political indoctrination classes, during which recruits were familiarized with Soviet history and Marxist-Leninist ideology. Training and indoctrination activities were carried out for 6 days a week. On Sundays, the recruits were responsible for maintaining the equipment and weapons, as well as the barracks where the training took place, being directly responsible for how the sleeping and dining areas were maintained (Ib., p. 10).

RATIONS

Unlike the diet of infantrymen in other European armies, the diet of the Soviet infantryman was as frugal as possible. While the recruit was in training, he was provided with three meals a day. For breakfast, a type of wheat porridge called *cașa* was served, lunch consisted of a plate of borscht, and for dinner, the soldiers received bread and pickles (Lucas, 2014, p. 83). This diet provided the minimum calories necessary for soldiers in peace time. The situation changed, however, when the troops were on long marches and on the offensive, as was the case during the invasion of Bessarabia, when *“the food was reduced and very little, consisting of (sic!) most days of boiled and slightly sugared tapioca, which (sic!) made everyone very weak and pale in appearance.”* (A.M.R.P., 1940, p. 15).

EQUIPMENT WITH WEAPONS AND AMMUNITION

In the context where the recruits came mainly from rural areas and did not have higher education, which would familiarize them with advanced principles of mechanics, the armament provided was simple, robust and easy to use by any soldier with minimal theoretical training. The basic weapon of the Soviet rifleman was the Mosin Nagant M1981 rifle. In service since Tsarist times, this 7.62 mm caliber weapon was very widespread in the Red Army, mainly due to the huge stocks left over from World War I. With a length of 123.2 cm and a 5-round magazine, the efficiency of this weapon was comparable to the Z.B. M1930 in service with the Romanian infantry. To support the infantry actions, the Degtyarev Pakhotnyi light machine gun of 7.62 mm caliber was used. With a 47-round drum magazine, used efficiently, it could have a rate of fire of 500-600 rounds per minute. But since conditions in combat are rarely favorable, in practice the rate of fire was only 80 rounds per minute.

The Soviet infantryman was also equipped with a wide range of grenades. Among them were the F-1 fragmentation grenades, unconventionally called limonka-lemon, due to its shape, the RG-42 and the RGD 33. In addition to these, there were also bottles with a flammable mixture, similar to the famous Molotov cocktails of Finnish origin (Rottman, pp. 24-28).

The ammunition for the Mosin rifle was stored in cartridge cases located on the belt, they contained 40 cartridges, and in the shoulder strap there were another 14 sectors, each of 5 cartridges. Most often, a bayonet was also attached to the weapon. For protection against shrapnel, soldiers were equipped with various

types of Soviet-made helmets. The infantryman's equipment included M36, SSch-39 and SSch-40 helmets. Often, the helmet was attached to the backpack, the soldier preferring to wear Pilotka, a type of olive-green textile cap. Other personal effects were stored in the back pack or gas mask bag (Campbell, 2014, pp. 41-42).

ORGANIZATION OF RIFLE TROOPS

The Soviet infantryman was generically called a rifleman, which is why he was part of rifle units and subunits, not infantry men, as is the case in other armies. This semantic difference is related to the Russian tradition, according to which a rifleman (strelitsi) is more professional than a simple infantry man (pyekhoty) (Zaloga, p. 4). Following the difficulties encountered in the Winter War (Soviet-Finnish War), the rifle divisions were in the midst of reorganization in June 1941. Thus, a rifle group was to be formed by 11 soldiers. Four rifle groups formed a platoon, which was led by an officer and 2 non-commissioned officers. Three platoons formed a rifle company, to which was added a political commissar for a total of 5 officers and 171 soldiers. A rifle battalion was mainly composed of 3 rifle companies and had a total of 636 soldiers on paper. These three battalions formed, in turn, a rifle regiment, which could count 3,182 soldiers, of which: 131 were officers, 56 were political commissars, 435 were non-commissioned officers, and 2,560 were soldiers of various ranks (Campbell, 2014, pp. 124- 125). According to the new directives of April 1941, a rifle division counted on paper 14,483 soldiers (Askey, 2008). The divisions were, in turn, grouped into armies arranged in fronts, depending on the geographical area in which they carried out their activity.

CONCLUSIONS

The training and equipping of the Soviet infantryman continues to be a broad, complex subject of major importance for understanding the dynamics of military conflicts during World War II. This field requires and deserves to be approached with methodological rigor, scientific seriousness, and a detailed analysis of historical sources, in order to provide a faithful and comprehensive picture of the training process of Soviet soldiers, as well as of the military equipment and techniques used.

In military art, knowing your opponent is one of the fundamental pillars for achieving success and, implicitly, victory in armed confrontations. This idea emphasizes the importance of studying the enemy's strategy, tactics, resources, and mentality in order to effectively anticipate and counter his actions on the battlefield.

Currently, Romanian military historiography is making concentrated efforts to recover and adequately render the four decades in which Operation Barbarossa was a taboo subject, thus being eclipsed in the official and academic discourse. In this sense, numerous researches and publications try to fill the gaps in the collective memory, offering more balanced perspective on the events and the actors involved, as well as on their impact on the course of the Second World War.

For a comprehensive understanding of this event with a decisive impact on world history, it is necessary, however, to turn our gaze to the opposite side, which, from a historiographical point of view, continues to be shrouded in fog. Romanian scientific works, in general, frequently fail to provide an exhaustive perspective on the opponent on the left bank of the Prut, which limits in-depth knowledge of the structure, tactics and mentality of the Red Army. In this context, a notable contribution is Pavel Moraru's work – *"Stalin's Army as Seen by the Romanians"*. This book brings to the fore a reinterpretation of the image of the Soviet army in World War II, offering a different perspective from that conveyed by war propaganda and official Soviet historiography. Through a critical and documented analysis, the author reconstructs how the Soviet army was perceived by Romanians, thus contributing to a more nuanced understanding of the adversary and the mechanisms of propaganda and perception in the context of the conflict. In my opinion, this work represents an important step in diversifying and deepening knowledge about the Soviet forces and about how they were interpreted and understood from the Romanian perspective, being a valuable resource for a detailed study of the complexity of the Romanian-Soviet relationship during the war.

BIBLIOGRAPHY:

1. Romanian Military Archives Pitești/A.M.R.P., Collection 21 Infantry Division, 1940, File no. 2284, no. 846, f. 15, 25.
2. Askey, N., *Soviet Rifle Division 5th of May 1941*, <https://operationbarbarossa.net/wp-content/uploads/2014/06/TOE-Sov-RD-Apr-1941-1.pdf>, retrieved on 31 August 2025.
3. Campbell, D. (2014). *German Infantry man versus Soviet Rifleman*. Oxford: Editura Ospery Publishing.
4. Constantiniu, F. (2011). *O istorie sinceră a poporului roman*. București: Editura Enciclopedic Gold.
5. *Constituția Sovietică din 1936*, <https://www.marxists.org/history/ussr/government/constitution/1936/1936-constitution.pdf>, retrieved on 30 August 2025.
6. Lucas, J. (2014). *War on The Eastern Front, The German Soldier in Russia 1941- 1945*. Londra: Editura Frontline Books.
7. Moraru, P. (2006). *Armata lui Stalin văzută de români*. București: Editura Militară.

8. Rottman, G.L. (2007). *The Soviet Rifleman 1941-1945*. Oxford: Osprey Publishing.
9. Schechter, B.M. (2015). *The Material Culture of the Red Army 1941-1945*, Berkeley.
10. *The law "on the universal military duty"*, <https://www.prilib.ru/en/history/619624>, retrieved on 30 August 2025.
11. Zolota, S.J. (1984). *The Red Army of the Great Patriotic War 1941-45*. Oxford: Editura Osprey Publishing.
12. <https://www.prilib.ru/en/history/619624>, retrieved on 30 August 2025.

ROMANIAN-AMERICAN RELATIONS IN THE NAVAL FIELD (1975-1980)

Navy Captain Dr. Marian TĂNASE, BEng

Commanding Officer of the 39th Divers Center

DOI: 10.55535/RMT.2025.3.44

In the summer of 1975, the destroyer "WAINWRIGHT" of the US Navy's Sixth Fleet in the Mediterranean conducted a 4-day port call at the Port of Constanta. This marked the first official courtesy visit of a US Navy vessel to a Romanian port in 49 years. The previous visit of a US vessel had been that of the "SCORPION" yacht in 1926.

The visit of a US naval vessel – the world's leading maritime power and the leader of NATO – to Romania – a member of the Warsaw Pact –, conducted almost one month after the USA and the USSR had marked 30 years since the end of World War II through a reciprocal exchange of vessels, was a significant political, diplomatic and social event, considering the time and context in which it was organized.

In the following years, until 1989, the port call at Constanta of a US naval vessel, followed by two other port calls, became an annual reference point in the US-Romanian diplomatic and military relations, despite the fact that the two states were members of alliances with fundamentally different ideologies.

Keywords: Romanian-American relations; Romanian Navy; diplomatic impact; military relationship; Warsaw Pact;

INTRODUCTION

In the summer of 1975, a high-level meeting was organised between Romania and the USA. Between 7 and 11 June 1975, Romanian President Nicolae Ceaușescu visited Mexico, but before flying back to Europe he met US President Gerald Ford in Washington on 11 July 1975. The two presidents met again at the end of the same month in Helsinki during the Conference on Security and Cooperation in Europe. The following day after signing the *Final Act*, on 2 August 1975, the US President arrived in Bucharest for an official visit.

Between these two events, the first port call of a US Navy vessel was conducted in the Romanian port of Constanța, after 49 years after the last such visit. Before this port call, the last US Navy vessel to arrive in Constanța was the yacht “SCORPION” in 1926.

Since 1914, for more than a decade, the “SCORPION” had been stationed in Istanbul and served as the flagship of a US admiral responsible for eastern affairs.

Through diplomatic efforts, the two parties agreed to organise the first “*courtesy visit*” of a US Navy vessel deployed in the Mediterranean between 20 and 24 June 1975. The ship designated to execute this naval diplomacy event was the destroyer “WAINWRIGHT” (DLG-28). She was a “BELKNAP”-class destroyer, in service with the US Navy since 1966, and was taken under the Sixth Fleet operational control in mid-March 1975.

Between 1975 and 1989, the focal point of US-Romanian relations in the naval domain were represented by an annual program of visits by US Navy vessels to Constanta. After 1990, in a different geopolitical and geostrategic context, US-Romanian relations gradually improved and became a major component of the bilateral relationship between the two states.

We can therefore state *that the year 2025 marks 50 years of uninterrupted naval relations between Romania and the USA.*

ASPECTS OF ROMANIAN-AMERICAN RELATIONS (1970-1975)

After Romania joined the UN and normalised its relations with the USA, Romanian diplomats in New York had the opportunity to interact with their American counterparts. The diplomatic efforts of Romanian diplomats, the foreign policy principles they promoted, as well as Romania’s distinct position within

the Warsaw Pact – different from that of the alliance's dominant power – favoured Romania's approach to the USA.

The dynamics of diplomatic, economic and political relations between Romania and the USA took an upward turn after President Richard Nixon visited Bucharest in August 1969 (*Scînteia*, anul XXXVIII, nr. 8145 and 8146, 3 and 4 August 1969, pp. 1-2). This was the first visit by an American president to a communist state. The visit took place amid tensions between Romania and the USSR, after the Warsaw Pact forces invaded Czechoslovakia the previous year.

This was followed by Nicolae Ceaușescu's visit to the USA between 4 and 6 December 1973. The joint political declaration signed by Richard Nixon and Nicolae Ceaușescu on 5 December 1973 expressed political and economic support for Bucharest's foreign policy (*Ib.*, no. 9713, 6 December 1973, p. 1).

Romania's interest in obtaining substantial economic assistance from the USA – the leading power of the Western world – was immense. The discussions and negotiations held before and after August 1969, aimed at normalising and strengthening bilateral relations between the diplomats of the two countries, as well as the meetings between US Presidents Richard Nixon and Gerald Ford with Nicolae Ceaușescu, led to the signing of a series of diplomatic, cultural and economic agreements. Although carried out cautiously, but of significant importance to both sides, the military relations were accompanied by the diplomatic and economic ones.

After 1970, during bilateral negotiations, the issue of signing a military cooperation agreement was most likely raised, framed within the political context of that historical period. The USA and Romania belonged to different alliances with opposing ideologies, yet, Romania's behaviour in its relation with the USSR, its good ties with China, and its openness to cooperation with Western states encouraged the leadership in Washington to pay greater attention to Bucharest and its communist leader. In 1974, the foundations were laid for a rapprochement between the two armed forces through the signing of a military cooperation convention (Watts, 2012, p. 693). The following year, reciprocal high-level visits represented a genuine success of the foreign policies of both countries, each pursuing different objectives.

Between 11 and 20 March 1975, the Chief of the Romanian General Staff, Colonel-General Ion Coman, accompanied by a military delegation, paid an official visit to the USA at the invitation of the US Army Chief of Staff, General Fred C. Weyand (*Scînteia*, year XLIV, no. 10126, 12 March 1975, p. 5; no. 10130, 16 March 1975, p. 4). This was the first visit to Washington by a general from a member state of the Warsaw Pact. The visit was reciprocated by General Weyand in September 1975

(*Scînteia*, year XLIV, no. 10274, 2 September 1975, p. 4; no. 10277, 5 September 1975, p. 5; no. 10278, 6 September 1975, p. 6).

The issue of a US Navy vessel visiting Constanța must have been among the topics discussed between the Americans and General Coman. Since 1970, the Pentagon, the State Department and the US Navy had sought to have at least one ship sail north of the 44° N parallel during Black Sea deployments for reasons other than a “*Silver Fox*” mission, and an official visit to Constanța offered this opportunity.

On the other hand, two years after the opening of the *Conference on Security and Cooperation in Europe*, on 1 August 1975, the representatives of 35 countries signed the Final Act of Helsinki, the document that laid the foundation of the OSCE (*Official Bulletin*, no. 92, 13 August 1975). Romania was an active participant in this “*Euro-Atlantic congress*”.

Through the *Document concerning confidence-building measures and certain aspects of security and disarmament*, a number of obligations and recommendations were agreed upon, including reciprocal notification of large-scale military manoeuvres and the exchange of observers. The signatories were encouraged to promote “*invitation-based exchanges among their military personnel, including visits and military delegations.*” (Ib.). Both the Americans and the Romanians viewed these “*recommendations*” as an opportunity to elevate their bilateral political and military relations to a new level under the umbrella of the OSCE, even though each side pursued different objectives.

Between 1960 and 1974, isolated American ships or groups of two or four destroyers entered the Black Sea to signal naval presence and exercise the right of freedom of navigation as part of “*Silver Fox*” missions. The duration of their stay was generally three to four days. Starting in 1968, during their presence in the Black Sea, the navigation area of American ships was limited by the State Department to latitude 43°30'N (Tănase, 2024, pp. 63-78).

In this context, in the summer of 1975, reciprocal high-level visits took place between Romania and the USA. Nicolae Ceaușescu visited Mexico (7-11 June 1975) and, before flying back to Europe, “*made a short visit to Washington*”, meeting President Gerald Ford on 11 June 1975 (*Scînteia*, year XLIV, no. 10204, Thursday 12 June 1975, p. 1). At the end of the month, the two heads of state were in Helsinki to participate in the CSCE, which concluded with the signing of the Final Act, negotiated and agreed upon by a large number of states. The signing ceremony of the “*Final Act*” took place on 1 August 1975. The next day, President Gerald Ford visited Bucharest (*Scînteia*, Ib., no. 10248, 2 August 1975, p. 1; no. 10249, 3 August 1975, pp. 1-5).

Between these two events, diplomatic arrangements were made for a US ship from the Sixth Fleet in the Mediterranean Sea to pay a “*courtesy visit*” to Constanța between 20 and 24 June 1975. Thus, the destroyer USS “WAINWRIGHT” became the first American ship to visit Romania after almost 40 years (*Scînteia*, lb., no. 10212, 21 June 1975, p. 5; no. 10215, 25 June 1975, p. 3).

Another important event in the political-military relations between Romania and the USA was the visit to Bucharest of General Fred C. Weyand, from 1 to 5 September 1975 (*Scînteia*, lb., no. 10274, Tuesday 2 September 1975, p. 4.; no. 10278, 6 September 1975, p. 6), held almost a month after President Ford’s visit to the Romanian capital (*Scînteia*, lb., no. 10277, Friday 5 September 1975, p. 5). Shortly after the American General’s departure, on 8 September 1975, as the Americans were preparing the celebrations for the following year’s bicentennial of US independence, John William Middendorf II (Secretary of the Navy) sent a letter to the Chief of the General Staff, Colonel-General Ion Coman, inviting the training ship “MIRCEA” to an international parade organised for the occasion and to the “*race of the century*” – “*Operation Sail 1976*”.

The Romanian side accepted the invitation, and the training ship “MIRCEA” successfully represented Romania at the 3rd Bermuda – Newport race as part of “*Operation Sail 1976*” and at the festivities marking the bicentennial of the independence of the United States of America (Damaschin, 2006).

THE FIRST VISIT OF AN AMERICAN WARSHIP TO CONSTANȚA DURING THE COLD WAR

Romanian-American relations saw a significant improvement in 1975. For 15 years, the American naval presence in the Black Sea had been maintained through *Operation Silver Fox*. A visit by a warship to a port on the western coast of the Black Sea, namely the Romanian port of Constanța, had been considered by American diplomacy and the U.S. Navy since the autumn of 1970, as a response to Soviet actions in Cuba and as a way to extend the operational area north of the 43°30’ parallel.

While American destroyers had begun, during their patrols in the Black Sea starting in 1971, to reach points near the territorial waters of the USSR, the visit to Constanța took place in the summer of 1975. Through diplomatic arrangements, both sides agreed to schedule the “*courtesy visit*” of an American warship deployed in the Mediterranean between 20 and 24 June 1975. The ship designated for this act of naval diplomacy was the destroyer “WAINWRIGHT” (DLG-28). It was a “BELKNAP”-class guided missile destroyer leader, in service with the US Navy since

1966, which came under the operational control of the Commander of the Sixth Fleet in the Mediterranean in mid-March 1975.

The American destroyer received the mission to pass through the Turkish straits and, after entering the Black Sea, to head toward the port of Constanța at the beginning of June. The mission was regarded by the ship's crew as extremely important. "WAINWRIGHT" was to be the first American ship to enter the port of Constanța after 49 years (*All Hands*, 1975, p. 45).

The last visit of an American warship to Constanța had been that of the yacht "SCORPION" in 1926. Since 1914, for more than a decade, the "SCORPION" had been stationed in Istanbul and served as the flagship of a US admiral responsible for eastern affairs.

The "courtesy visit" of USS "WAINWRIGHT" began on the morning of Friday, 20 June 1975 (*Dobrogea Nouă*, 1975, p. 3). The American destroyer, commanded by Commander Eugene B. Ackerman, officially on a "cruise in the Black Sea", entered the port escorted by a Romanian naval vessel from the limit of Romanian territorial waters. After firing a 21-gun national salute, it moored at the quay of the Maritime Station in the port of Constanța.

Although time was very short, the Romanian side prepared intensely for the visit of a ship belonging to the world's greatest naval power. The training ship "MIRCEA" was designated as the host vessel, and the "Mircea cel Bătrân" Naval Institute was responsible for organising the reception of the American ship. For this purpose, "MIRCEA" was moved to a berth near the Maritime Station.



The destroyer USS "WAINWRIGHT" (DLG-28) during a mooring maneuver in the Port of Constanța. In the bow, the training ship "MIRCEA" can be seen moored at the quay.

Upon mooring, the destroyer *“WAINWRIGHT”* was welcomed on the quay by a delegation of naval officers, the American ambassador to Bucharest, Harry G. Barnes, and the US military attaché in Romania, Colonel Wyatt J. Mitchell.

Shortly after the mooring maneuver was completed, the commander of *“WAINWRIGHT”*, Commander Eugene B. Ackerman, accompanied by Harry G. Barnes and Wyatt J. Mitchell, paid a formal visit to the mayor of Constanța, Gheorghe Trandafir, and later to the training ship *MIRCEA*”, where he was received by the Commander of the Romanian Navy, Rear Admiral Sebastian Ulmeanu (Ciorbea, 1999, p. 205).

In 1975, the main naval base of the Romanian Navy was located in Mangalia. The Navy HQ, the HQs of the 42nd Maritime Division and the 29th Torpedo Boat Brigade, as well as the maritime and land units under their command, had their administrative headquarters within the Mangalia naval port. In the port of Constanța, where berth *“zero”* was under construction, a few ships belonging to the 306th Training Ship Division, subordinate to the *“Mircea cel Bătrân”* Naval Institute, were stationed, or were temporarily relocated from Mangalia for student training.

The protocol agreed upon by the two sides contained all the elements of an official courtesy visit, which later became reference points for the programs of future visits:

- greeting the American ship arriving for the visit at the entrance to territorial waters and escorting it to the port entrance by a Romanian naval vessel;
- entering the port and mooring at the berth in the morning of the first day of the visit;
- firing the national salute (21-gun salute) by the visiting ship upon entering the port. The response was given by an artillery battery positioned on the eastern breakwater/the outer breakwater;
- welcoming the ship and assisting with the mooring manoeuvre by representatives of the Romanian Navy and the US Embassy in Bucharest;
- boarding of the ambassador, the military attaché, and the liaison officer from the Romanian Navy;
- visits by the ship’s commander to the Constanța City Hall and to the Commander of the Romanian Navy (usually aboard the training ship *“MIRCEA”*);
- visits to the training ship *“MIRCEA”* and to the *“Mircea cel Bătrân”* Naval Institute by the American ship’s crew;
- visits to the American ship by groups of servicemen and civilians. On several occasions, civilian access to the American ships was restricted;

- a wreath-laying ceremony at the “Victory” Monument in the Archaeological Park of Constanța;
- sports competitions, usually volleyball and basketball matches, between teams from the ship’s crew and teams of students from the Naval Institute;
- organizing excursions for the American ship’s crew to visit Constanța and several resorts along the Romanian seaside.

The unit designated to act as host was most often the “*Mircea cel Bătrân*” Naval Institute, with the training ship “*MIRCEA*” serving as the host vessel. When “*MIRCEA*” was not present in the port, being away on training voyages, it was replaced by Hydrographic Ship 112 (formerly the gunboat “*STIHI*”).

In honour of the ship’s arrival, the US ambassador hosted a reception, usually held at the “*Cazino*” Restaurant on the Constanța seafront, though receptions were also held aboard American ships. The Romanian side, in turn, usually offered a lunch aboard the training ship “*MIRCEA*” and a return cocktail.

Beyond the political and diplomatic impact of the visit, perhaps the most important aspect was the fact that USS “*WAINWRIGHT*” was open to visitors, giving Romanian naval personnel and other citizens of Constanța the opportunity to interact with the ship’s crew and to see a large warship belonging to the world’s leading capitalist power.

The Romanian side organised a visit for the American crew aboard the training ship “*MIRCEA*”, as well as excursions to tourist sites along the Romanian Black Sea coast. Interaction between Romanian and American sailors also included friendly sports matches between the two sides. The visit of the destroyer “*WAINWRIGHT*” to Constanța ended on Tuesday, 24 June 1975 (*România Liberă*, year XXXIII, no. 9538, 25 June 1975, p. 5). This event of naval diplomacy was duly appreciated by both sides, each concluding that it was in their interest for this type of activity to continue in the years to come.

VISITS OF AMERICAN SHIPS TO CONSTANȚA IN 1976, 1977, AND 1978

During 1976, a total of five American ships entered the Black Sea. Between two periodic missions carried out by groups of two ships, an official visit to the port of Constanța took place (MacDonald, 1983, pp. 2-8). The second visit of an American ship to Romania occurred between 9 and 13 September 1976 (*Scînteia*, anul XLV, nr. 10593, 10 septembrie 1976, p. 5; nr. 10596, 14 septembrie 1976, p. 5). On the morning of 9 September 1976, the American cruiser “*HARRY E. YARNELL*”, with a crew of just over 400 sailors and commanded by Captain Richard C. Avrit, entered

the Port of Constanța, escorted by a Romanian naval vessel. Aboard the cruiser "YARNELL" was Rear Admiral Eugene J. Carroll, Jr., serving as commander of the deployment. An important military figure in the US Navy, he had, since 14 July 1975, held the positions of Task Force Commander (TF-60) and Carrier Group Commander (Carrier Group Two) within the US Sixth Fleet in the Mediterranean. Within NATO's force structure, he served as Task Force Commander (TF-502) (<https://www.navysite.de/cruisebooks/cv67-77/009.htm>).

From a naval diplomacy standpoint, Admiral Carroll's presence in Constanța represented a significant moment in bilateral relations. Most likely, this initiative was motivated, among other reasons, by the fact that during the celebrations held in New York to mark the 200th anniversary of the United States Declaration of Independence, Romania was represented by the training ship "MIRCEA". While stationed in American ports, "MIRCEA" had as deployment commander Rear Admiral Gheorghe Sandu, a former Navy commander who at that time served as head of the Navy Section within the Operations Directorate of the General Staff¹.

Eugene J. Carroll was the first American admiral to visit Romania in 50 years. During the inter-war period, Rear Admiral Mark Lambert Bristol, the US High Commissioner to Turkey in Constantinople between 1919 and 1927, had visited Romania in August 1926.

For the visit of the cruiser "HARRY E. YARNELL", as in the previous year, the "Mircea cel Bătrân" Naval Institute and the ship "MIRCEA" were designated as the host unit and host ship, respectively.

At 09:00 on the morning of arrival at the Maritime Station berth, the cruiser was awaited by a delegation of Romanian authorities and by representatives of the US Embassy in Romania: the chargé d'affaires Richard Noyes Viets, the military attaché Colonel Wyatt J. Mitchell, and the naval attaché Commander Russel Fredirk. After the welcome aboard, the deployment commander, Rear Admiral Carroll, and the cruiser's commanding officer, Commander Avrit, accompanied by Richard Noyes Viets and the two American attachés, paid a courtesy visit to the mayor of Constanța, Gheorghe Trandafir. They were then received by the Commander of the Romanian Navy, Rear Admiral Sebastian Ulmeanu, aboard the training ship "MIRCEA", where he offered a luncheon to the American guests (Ciorbea, p. 244). That same afternoon, a wreath-laying ceremony took place at the Victory Monument in the Archaeological Park of Constanța, conducted by Rear Admiral Eugene Carroll, accompanied by Commander Richard Avrit (*Scînteia*, year XLV, no. 10593, 10 September 1976, p. 5).

¹ The training voyage of the training vessel "MIRCEA" in 1976 took place between 4 March and 30 August, in Valentin Ciorbea, *op.cit.*, pp. 231-243.



Commander Richard C. Avrit, commanding officer of USS "Harry E. Yarnell" (CG-17), speaking on board the ship with Romanian officers during the American ship's visit to Constanța (September 1976)

During the visit, various tours, events, meetings, and sports competitions were organised. The American admiral visited the Naval Institute and most likely was taken to other economic and tourist sites in Dobrogea. Reciprocal receptions were held aboard the training ship "MIRCEA" and the American cruiser (Ciorbea, p. 244). The American sailors visited resorts, historical monuments, and cultural-touristic objectives along the Romanian Black Sea coast. The American ship was also open to visits by civilians, Romanian military and civil authorities, and Romanian sailors every afternoon from 10 to 12 September, for two hours each day.

The cruiser "HARRY E. YARNELL" departed the port of Constanța on the morning of Monday, 13 September 1976 (*România Liberă*, year XXXIV, no. 9918, 14 September 1976, p. 5).

During 1977, the Sixth Fleet in the Mediterranean conducted three missions to the Black Sea: two patrols and one official visit to Constanța.

In September 1977, the US Sixth Fleet in the Mediterranean sent the guided-missile destroyer "CHARLES F. ADAMS" (DDG-42) on an official visit to Constanța², marking its second presence in the Black Sea that year.

The visit (<https://www.navysite.de/dd/ddg2.htm>) took place between 8 and 12 September 1977 (*Dobrogea Nouă*, year XXX, no. 9028, 9 September 1977, p. 3; *Scînteia*, year XLVI, no. 10906, 13 September 1977, p. 3). The five-day program resembled that of the previous year: a welcome visit; protocol calls to local political and military authorities, the mayor of Constanța, the commander of the Romanian

² *Third Semiannual Report to the Commission on Security and Cooperation in Europe, June 1, 1977 - December 1, 1977*, no. 39, December 1977, Washington D.C., p. 7.

Navy, and the commander of the Naval Institute *“Mircea cel Bătrân”*; a wreath-laying ceremony at the Victory Monument; a luncheon offered by the commander of the Romanian Navy; visits to historical monuments and tourist sites; sports competitions between ship crews; visits to the destroyer by civilians; and a cocktail reception aboard the American destroyer.

In 1978, the US Sixth Fleet in the Mediterranean sent ships to the Black Sea twice. The first time, at the end of June, a cruiser and a destroyer carried out missions specific to Operation *“Silver Fox”*, and the second American presence in the Black Sea that year was an official visit to Constanța by an American cruiser at the end of November 1978.

In May 1978, American diplomacy proposed that the Silver Fox Mission in the Black Sea be carried out between 26 June and 1 July with the guided-missile cruiser *“HARRY E. YARNELL”* (CG-17) and the guided-missile destroyer *“CHARLES F. ADAMS”* (DDG-2). The mission was to be executed without a port visit (<https://ia600605.us.archive.org/23/items/StateDeptcable1978-131504/State%20Dept%20cable%201978-131504.pdf>).

According to the planned mission route, the American ships were to navigate no closer than 70 nautical miles from Romania, 50 nautical miles from Bulgaria, and 40 nautical miles from the coast of the USSR. The American ships were also scheduled to pass through training areas No. 3, 4, and 8, notified by the Soviets in the northern part of the Black Sea (Ib.).

The safety instructions established for the navigation of the American ships required them to avoid the Soviet Black Sea Fleet’s training areas if live-fire exercises were underway. To take advantage of opportunities to gather information on targets of interest, ship commanders were authorised to deviate from the planned route for more than four hours; however, the ships were not allowed to approach closer than 15 nautical miles from a coast or island, in order to avoid entering the territorial waters of any of the target countries (Ib.).

The second American naval presence in the Black Sea in 1978 took place in a particularly sensitive political climate and demonstrated political support for Romania in its relations with the USSR. USS *“BIDDLE”* (CG-34) was stationed in Constanța between 22 and 27 November 1978 for a six-day official visit to Romania (Ib.).

Romanian-American relations in 1978 were marked by three significant events: Nicolae Ceaușescu’s visit to Washington (12-17 April 1978); the granting of political asylum in the United States to Ion Mihai Pacepa (late July 1978); the *“personal*

message” from Jimmy Carter to Nicolae Ceaușescu, transmitted through the US Secretary of the Treasury during his unexpected visit to Bucharest (December 1978)³.

Ceaușescu’s visit to the United States in the spring of 1978 was considered a genuine success of Romanian foreign policy and was widely reported in the central press in Bucharest. The “*joint declaration*” on international issues and bilateral relations, issued at the conclusion of the talks between the two heads of state, reaffirmed the political and economic support of the United States for Romania (*Scînteia*, year XLVII, no. 11087 ÷ 11091, 13 ÷ 18 April 1978).

In the summer of 1978, three months after the meeting between Carter and Ceaușescu, relations between Romania and the United States entered a crisis triggered by the request for – and granting of – political asylum in the US to General Ion Mihai Pacepa, head of the Romanian foreign intelligence service, through the American Embassy in Bonn (FRG). The defection on 24 July 1978 of Pacepa, the chief of the communist regime’s spies and a close associate of the Ceaușescu family, created tensions between the Americans and the Romanians. However, it did not immediately cause the two sides to abandon their political, diplomatic, economic, or military relations. The effects appeared gradually over time.

Between 22 and 23 November 1978, the Consultative Political Committee of the Warsaw Pact held a conference in Moscow. Coincidence or not, on the very day the CPC meeting began in Moscow, USS “*BIDDLE*” docked in the port of Constanța. At this summit, Nicolae Ceaușescu opposed Marshal Kulikov’s proposals regarding increased military spending and command-and-control arrangements in the draft statute of the Unified Armed Forces for wartime. At the conclusion of the conference, it was intended that two declarations be issued: one concerning the situation in Europe and the international situation as a whole, and a second concerning the situation in the Middle East.

The Romanian delegation did not agree with the declaration on the Middle East, which aimed to issue a collective condemnation – under the aegis of the Warsaw Pact – of the Camp David Accords and Egypt’s separate peace with Israel, as well as to support the Arab states that, at their Baghdad summit, had decided to exclude Egypt from the Arab League following President Sadat’s “*betrayal*” of Arab interests.

Although Romania did not agree with a separate peace between Egypt and Israel without the participation of the other parties, it supported the Camp David

³ See: *Foreign Relations of the United States, 1977-1980*, Volume XX, *Eastern Europe*, United States Government Publishing Office, Washington, 2015, Documents 177-234, pp. 527-749.

Accords. As a result, the Warsaw Pact could not issue a common declaration on this issue, as desired by Moscow. Consequently, the declaration on the Middle East was published in the press of all other member-state capitals – except Bucharest (*Scînteia*, year XLVII, no. 11278, 24 November 1978, pp. 3-4).

This situation was perceived in Washington as a strong manifestation of Romania's independence from Moscow, revealing a new moment of tension between the leadership in Bucharest and those of the other Warsaw Pact states, especially the Soviets. This led the Carter administration to send an urgent message of support to Nicolae Ceaușescu, which arrived on 8 December 1978.

In mid-November, the guided-missile cruiser *"BIDDLE"* (CG-34) received the mission to conduct a visit to Constanța between 22 and 27 November 1978, carrying on board, as flag officer, Rear Admiral Paul D. Tomb, commander of Submarine Group 8 and commander of Mediterranean Submarine Forces (Treadway, 2005, p. 198).

On 20 November 1978, the American cruiser entered the Greek port of Piraeus (Athens), where Rear Admiral Tomb boarded. After passing through the Dardanelles and Bosphorus straits, on 21 November 1978, *"BIDDLE"* entered the Black Sea, and the next morning, Wednesday, 22 November, reached Romanian territorial waters, where it was escorted by a Romanian naval vessel to the entrance of the port of Constanța (Ib., p. 200). After rendering the national salute at the port entrance, the impressive American cruiser *"BIDDLE"* docked at the Maritime Station berth for a six-day official visit to Romania (*Scînteia*, year XLVII, no. 11277, 23 November 1978, p. 5; no. 11.281, 28 November 1978, p. 5). At the quay, the ship was greeted by a delegation of Romanian sailors and by the US ambassador to Bucharest, accompanied by the US military and naval attachés.

Immediately after mooring, the commanding officer of *"BIDDLE"*, Commander John N. Ryan, accompanied by the American military attaché, Commander Richard J. Wouakh, and five officers from the crew, paid a welcome visit to the training ship *"MIRCEA"*. The American officers were received by Rear Admiral Ștefan Ilie, commander of the Naval Institute. The training ship *"MIRCEA"* was moored near the Maritime Station (Ciorbea, p. 258).

The American delegation paid protocol visits to civilian and military authorities in Constanța. The American historian James A. Treadway remarked that *"Admiral Tomb, Captain Ryan, other Biddle officers, and the Defense Attaché Bucharest made official calls on a long list of Romanian dignitaries"* (Treadway, p. 200). In the Romanian press, only the protocol visits to the mayor of Constanța

and the commander of the Romanian Navy were mentioned (*Dobrogea Nouă*, year XXXI, no. 9 402, 23 November 1978, p. 4).

After the official visits to the political and military authorities, a wreath-laying ceremony took place at the Victory Monument in Constanța, carried out by Rear Admiral Paul Tomb and Commander John Ryan and attended by 40 members of the American ship's crew (Treadway, *ib.*). The Romanian side participated with a similar formation, ensuring the necessary conditions for the ceremony.

On the same day, the Romanian side offered a luncheon on board the training ship "*MIRCEA*", attended by Rear Admiral Paul Tomb, Commander John Ryan, Rudolph Aggrey, the US ambassador to Romania, Commander Richard J. Wouakh, the American military attaché, Commander Burton Weisman, the US naval attaché in Yugoslavia and Romania, and four other officers from the ship, representing the visitors; and by Rear Admiral Sebastian Ulmeanu, commander of the Romanian Navy, Rear Admiral Ștefan Ilie, commander of the Naval Institute, Captain (2nd rank) Dan Stăiculescu, commander of the training ship, and other officers, representing the Romanian side (Ciorbea, p. 258).

During the other five days of the "*BIDDLE*" cruiser's stay in the port of Constanța, various meetings, sports competitions, visits, and protocol activities took place ("*There was a reception; There were tours and general sightseeing in the city as well as numerous luncheons, sport competitions and cocktails*") (Treadway, *ib.*). The Romanian press only mentioned that "*the American sailors visited historical monuments and cultural-tourist sites on the Romanian Black Sea coast*" (*Scînteia*, year XLVII, no. 11281, 28 November 1978, p. 5).

We do not have information on whether the "*BIDDLE*" cruiser was opened for visits by the civilian population, but we believe this did not happen in December 1978, since such a protocol event would have generated major interest and would likely have been mentioned in the ship's monograph. It is possible that the Romanian side did not agree to such an activity, given that only a few months earlier the Pacepa event had taken place, creating major tension between Romanians and Americans. Nonetheless, "*BIDDLE*" was visited by groups of Romanian sailors and by local political and military officials, and receptions and cocktails were organised on board, attended by officials and other Romanian naval officers.

On Monday morning, 27 November 1978, after the farewell protocol visit carried out on board the training ship "*MIRCEA*", "*BIDDLE*" performed the unmooring manoeuvre and departed from the port of Constanța, leaving Romanian territorial waters and heading toward the Bosphorus Strait (Treadway, *ib.*).

Ten days later, on Thursday, 8 December 1978, Michael Blumenthal, the US Secretary of the Treasury, *“the envoy of the President of the US,”* arrived in Bucharest to deliver a *“personal message”* from President Carter to Nicolae Ceaușescu (*Scînteia*, year XLVII, no. 11287, 5 December 1978, p. 4; no. 11289, 7 December 1978, p. 6). After landing at Otopeni Airport, the American official told the press: *“I came to Romania at President Carter’s request to reaffirm to the Romanian people and to President Ceaușescu the importance we attach to **Romania’s independence** and to **Romanian-American friendship.**”* (Ib., no. 11290, 8 December 1978, p. 5; no. 11291, 9 December 1978, p. 5; no. 11292, 10 December 1978, pp. 1; 5; The Washington Post, 9 December 1978; The New York Times, 10 December 1978).

“BIDDLE”’s visit to Constanța was considered by both sides a success (*“significant diplomatic event”*) (Treadway, Ib.) It can also be seen as support offered to Nicolae Ceaușescu by American diplomacy in his dispute with the Soviet leadership in Moscow.

THE FIRST VISIT OF A GROUP OF TWO US NAVY WARSHIPS TO CONSTANȚA (1979)

Starting in the summer of 1979, the US Navy began making visits to Constanța with two ships (*“multi-ship US Navy visit to Constanța”*). Typically, these visits involved a cruiser and a destroyer serving with the US Sixth Fleet in the Mediterranean. This change can be seen as an increased display of the United States’ interest in the Black Sea region.

Maintaining a military relationship with Romania at a high diplomatic level, under the umbrella of the Confidence-Building Measures contained in the Helsinki Final Act, gave the United States the opportunity to continue showing support for Romania’s position within the Warsaw Pact, even though tensions existed between Washington and Bucharest regarding human rights issues in Romania, the granting of political asylum to the former head of the Foreign Intelligence Directorate of the Securitate, General Mihai Pacepa, and the level of economic exchanges (the annual renewal of the *“most favored nation” clause*)⁴.

The first visit to Constanța with two ships took place in June 1979, the two ships being the cruiser *“RICHMOND K. TURNER”* (CG-20) and the destroyer *“LAWRENCE”*

⁴ *“Two U.S. Navy ships visited Constanta, Romania, from June 22 – 25, 1979 [correct dates 18-25 author’s note.]. In addition, two U.S. Army War College students visited Poland, Hungary, and Romania during September and October 1979”*. Cf. United States Department of State, Bureau of Public Affairs, *Seventh Semiannual Report by the President to the Commission on Security and Cooperation in Europe on the Implementation of the Helsinki Final Act*, June 1, 1979 – November 30, 1979, Special report no. 62, 1979, Washington D.C., p. 9.

(DDG-4)⁵. On this occasion, the commander of the group was Rear Admiral William M. Callaghan Jr., the commander of the US Navy's Mediterranean Air Fleet.

For the cruiser "*RICHMOND K. TURNER*", this was its third and final entry into the Black Sea, and for the destroyer Lawrence, it was the only time it ever sailed in the Black Sea. Both American ships visited Romania only on this occasion. The two American ships stayed in Constanța for seven days. They arrived on the morning of Monday, 18 June, and departed on the morning of Monday, 25 June 1979 (*Scînteia*, year XLVIII, no. 11.453, Tuesday 19 June 1979, p. 5; no. 11.459, Tuesday 26 June 1979, p. 5; *Dobrogea Nouă*, year XXXII, no. 9578, Tuesday 19 June 1979, p. 4). This was the longest stay of US Navy ships in Romania during the period 1975-1990. They entered the Black Sea not for other dedicated missions, but solely to sail from Istanbul to Constanța and back, and to remain in the port of Constanța.

"*TURNER*" and "*LAWRENCE*" were met at the pier by officials from the United States Embassy in Bucharest and by representatives of the Romanian Navy. Some of them boarded the ships for the welcome visit: "*When the two ships tied up at the pier, crewmen found their quarterdecks busy with visitors, among them, American Ambassador ... Rudolph Aggrey*"⁶.

Most likely, the American crews had the opportunity to see the training ship "*MIRCEA*", either in port or outside the port, since it departed that same day for its annual training voyage in the Mediterranean and for official visits to the ports of Istanbul, Livorno, Lisbon, and Piraeus (18 June – 28 July 1979).

At that time, the Romanian Navy did not have combat ships in the port of Constanța, and the Navy Command was still located in Mangalia. In the port were the ships and diver boats of the Diving Center, and the hydrographic ship 112 (formerly the gunboat "*Lt. Cmdr. Eugen STIHI*") of the Maritime Hydrographic Directorate. Given this situation, the new diver boats were designated to carry out the mission of greeting the American ships upon entry into Romanian territorial waters and escorting them into the port, as well as guiding them upon departure, from the port to the exit from Romanian territorial waters. This practice became permanent for both American ships and other foreign naval vessels visiting Constanța in the following period.

As in previous years, the host unit from the Romanian Navy responsible for organizing and coordinating the visit of the American ships was the "*Mircea cel Bătrân*" Naval Institute. Starting the following year, however, commanders of the US

⁵ "18 June: The Sixth Fleet Ships *Richmond K. Turner* (CG 20) and *Lawrence* (DDG 4) began the first multi-ship U.S. Navy visit to Constanta, Romania". Cf. *Naval and Maritime Events*, 1979.

⁶ Lt. Mark E. Brender, *Romania Visit: The Celery Stumped Them. American Sailors Spend Seven Days in Romania in All Hands*, Magazine of the U.S. Navy, 57th year of publication, No. 756, January 1980, pp. 13 – 16.

Sixth Fleet holding the rank of Vice Admiral began visiting Constanța, and the host unit was designated as the 42nd Maritime Division, a large unit whose commander's position was assigned the rank of Vice Admiral. The vessel used to receive the American officials arriving for the visit was the hydrographic ship 112, replacing the training ship "MIRCEA" when the latter was in the port of Constanța and not away on its annual training voyage.



US Navy vessels moored in the Port of Constanța

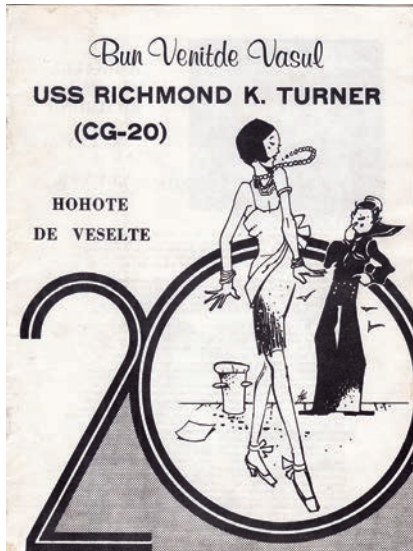
After the ships moored, the commander of the cruiser "TURNER", Commander Roger O. Simon, and the commander of the destroyer "LAWRENCE", Captain Commander Leo Anthony Cangianelli, were received on board the hydrographic ship 112 for the welcome visit by the commander of the Naval Institute, Rear Admiral Ștefan Ilie.

On the same day, Rear Admiral Callaghan, accompanied by the commanders of the two ships, Ambassador Rudolph Aggrey, and other American officers, paid protocol visits to the mayor of Constanța, the commander of the Romanian Navy, Rear Admiral Ioan Mușat, and the commander of the "Mircea cel Bătrân" Naval Institute, Rear Admiral Ștefan Ilie (*Scînteia*, year XLVIII, no. 11453, Tuesday 19 June 1979, p. 5; *Dobrogea Nouă*, year XXXII, no. 9578, Tuesday 19 June 1979, p. 4.). Most likely, on the day of arrival, the Romanian side hosted a luncheon.

On the afternoon of 18 June 1979 or the following day, a wreath-laying ceremony took place at the Victory Monument in Constanța, conducted by Rear Admiral William M. Callaghan Jr., accompanied by the two ship commanders. The ceremony involved detachments of Romanian and American sailors (Ib.).

Press releases in the Romanian media regarding the visit of the American ships were, as usual, brief, mentioning only a few aspects (*Scînteia*, year XLVIII, no. 11.453, Tuesday 19 June 1979, p. 5; no. 11.459, Tuesday 26 June 1979, p. 5). While in 1975 the American Navy's press featured only a short note about the visit of the cruiser "WAINWRIGHT" (DLG-28), this time, for the first time, the visit of the Sixth Fleet ships to Constanța was described in the most popular publication of the US Navy ("All Hands": Magazine of the U.S. Navy) (Brender, Ib.).

An important element of the visit program was the agreement to allow the civilian population of Constanța and Romanian Navy sailors to visit the cruiser "RICHMOND K. TURNER" and the destroyer "LAWRENCE", based on approximately 2,000 tickets made available by the Americans through the Romanian authorities. Romanians showed great interest, which made a strong impression on the Americans.



The flyer provided by the ship's crew to Romanian visitors



Aspects of the wreath-laying ceremony

Among the other protocol activities, one can mention the reception held on board the two ships, attended by 65 guests – local political and military officials, including the mayor of Constanța and the commander of the Romanian Navy, as well as "other local VIPs". Representatives of the American embassy in Bucharest and their invited guests were also present. During the reception, the atmosphere was enlivened by "The Hurricanes", the band of the "TURNER"'s crew.

For the first time, the command of the U.S. Sixth Fleet in the Mediterranean sent its musical group, the "Diplomats", to Constanța on a special military transport. They performed

concerts at the “*Mircea cel Bătrân*” Naval Institute and at the headquarters of the 9th Mechanized Infantry Division “*Mărășești*”. These activities were well appreciated by both Romanians and Americans. This type of activity became a regular feature in the program of visits in the following years.

For six days, the sailors followed a schedule that included official activities, sports competitions, organised tours, and visits around the city of Constanța and the seaside resort of Mamaia⁷.

The impressions of the crew members of the two ships regarding their visit to Romania, recorded in the article published in the US Navy magazine, are noteworthy (Ib.):

„I never thought I'd ever see a Communist country”.

„When I went ashore, I didn't really know what to expect or how the people would treat me”.

„As it turned out, the Romanians were really curious about our ship and our perceptions of their country”.

„At first, they were a bit standoffish and didn't know how to approach us”.

„Things were pretty controlled by the Romanian Navy and government security officials”.

„We've always been told that sailors are ambassadors of good will for our country. When you visit a country like Romania and wear your uniform ashore, you can see just how important we really are in helping our government make friends around the world”.

The cruiser “*RICHMOND K. TURNER*” (CG-20) and the destroyer “*LAWRENCE*” (DDG-4) departed from the port of Constanța on the morning of Monday, 25 June 1979, assisted during the unmooring manoeuvre by Romanian and American officials (*Scînteia*, year XLVIII, no. 11.459, Tuesday 26 June 1979, p. 5). This was the longest period that US Navy warships remained in the port of Constanța during the entire Cold War (8 days).

⁷ The Romanian press release states that: “During their stay in our country, the crew members of the two ships visited historical monuments and cultural-tourist sites in the city of Constanța and along the Romanian Black Sea coast”. *Scînteia*, year XLVIII, no. 11.459, Tuesday 26 June 1979, p. 5. The article by the American officer in All Hands describes the activities of the crews as follows: “While some of the Navymen toured museums, Greek and Roman ruins, and a winery, others chose to watch a folk show, dine at tempting restaurants, and talk with English and Irish tourists at Western-style discotheques. The resort area, state-owned and managed, attracts tourists from all over Europe. During the height of the season, the resort hotels accommodate almost 50,000 visitors. About 75 retired Americans live in Romania and, according to the American Embassy in Bucharest, about 28,000 U.S. tourists visited last year. Even with all the English-speaking tourists, many signs and menus are printed in still other languages. During the seven-day stay, the beautiful resort beaches of Mamaia enticed many swimmers and sunbathers. Enjoying 85-degree temperatures, the American sailors found the beach their favorite liberty spot....Before their visit to Constanta ended, the Americans joined men from the Romanian Navy in soccer, basketball and volleyball games.”, Ib.



Aspects of the visits to the American warships

One month later, the cruiser “*RICHMOND K. TURNER*” successfully launched the US Navy’s new missile, the well-known Harpoon, in the Gulf of Sidra. The missile hit and destroyed a naval target at a distance of 78 nautical miles (126 km). The *TURNER* was the first US Navy ship deployed to carry out a launch of this type of missile (https://en.wikipedia.org/wiki/USS_Richmond_K._Turner).

Starting in the summer of 1979, the destroyer *CARON* (DD-970), equipped with advanced intelligence-gathering systems, primarily in the electromagnetic spectrum, was sent to the Black Sea. In the second half of 1979, *CARON* carried out two missions in the Black Sea. During its first deployment, from 1-6 August 1979, it was accompanied by the destroyer “*FARRAGUT*” (DDG-37), and during the second deployment, from 12–16 October 1979, it was accompanied by the frigate “*MACCANDLESS*” (FF-1084)⁸.

CONCLUSIONS

Between 1975 and 1978, one US Navy warship visited Constanța each year, and in the following ten years, the annual visit was carried out by a group of two ships.

The opening established in 1975 had an important impact on US-Romanian relations. Naval diplomacy, exercised by each side through the visit of American ships to a Warsaw Pact country and through Romania’s reception of vessels from the world’s greatest maritime power and the undisputed leader of Western democracies, played a significant role.

⁸ “The Caron (DD 970) and the Farragut (DDG 37) entered the Black Sea for five days of routine operations in international waters. The Associated Press reported that while they were in the Black Sea, Soviet aircraft, including the Backfire bomber, simulated missile attacks on the two Sixth Fleet ships.” Cf. *Naval and Maritime Events 1979*.

This type of relationship between the US and socialist Romania, even if formally placed under the umbrella of the CSCE, gradually developed and survived political tensions between the two states, including the US granting asylum to General Mihai Pacepa, one of the leaders of the Romanian “*Securitate*” (1978), and the granting/ waiving of the most-favored-nation clause in the context of human rights violations by the Bucharest regime (1988).

At least for the period 1975-1978, with regard to US relations with East European countries, whether members of the Warsaw Pact or not, American diplomacy considered that most “*military exchanges*” took place with Romania⁹.

For each annual visit to Romania of US Sixth Fleet ships from 1976-1989, the US Navy was represented by an admiral; on several occasions, this was the fleet commander himself. In total, 11 admirals represented the US Navy during naval diplomacy activities in Constanța.

Of the eight commanders of the US Sixth Fleet during this period, five visited Constanța: Vice Admirals William H. Rowden (1982 and 1983), Edward H. Martin (1984), Frank Kelso II (1985 and 1986), Kendall E. Moranville (1988), and James D. Williams (1989). As can be seen, Vice Admirals Rowden and Kelso visited Romania twice, in consecutive years. The other six American admirals who set foot on Romanian soil were Rear Admirals Eugene J. Carroll, Jr. (1976), Paul D. Tomb (1978), William M. Callaghan Jr. (1979), Joseph Metcalf III (1980), Henry C. Mustin (1981), and Roger F. Bacon (1987).

In conclusion, naval diplomacy activities had a significant impact on bilateral relations, facilitating communication and cooperation between the two states despite political tensions and the geopolitical context of the Cold War. Moreover, the visits represented an essential element of US naval diplomacy, strengthening the position of the United States in its relations with socialist Romania and contributing to the maintenance of established contacts despite a tense political context.

BIBLIOGRAPHICAL REFERENCES:

1. *All Hands*, Magazine of the U.S. Navy, nr. 704, September 1975, p. 45.
2. Lt. Brender, M.E. (1980). *Romania Visit: The Celery Stumped Them. American sailors spend seven days in Romania*, in *All Hands*, Magazine of the U.S. Navy, 57th year of publication, No. 756, January, pp. 13-16.
3. *Buletinul Oficial*, nr. 92, 13 august 1975.
4. Ciorbea, V. (1999). *Istoricul navelor școală “Mircea”*, vol. 2. Constanța: Editura ANMB.
5. Damaschin, I. (2006). *Cu “Mircea” pe drumul lui Columb*. București: Editura Capitel.

⁹ *Fulfilling Our Promises: The United States and the Helsinki Final Act*, Washington, 1979, pp. 315-316.

6. *Dobrogea Nouă*, anul XXVIII, nr. 8341, 21 June 1975, p. 3; year XXX, nr. 9028, 9 September 1977, p. 3; year XXXI, nr. 9 402, 23 November 1978, p. 4; year XXXII, nr. 9578, Tuesday 19 June 1979, p. 4.
7. *Foreign Relations of the United States, 1977-1980*, vol. XX, *Eastern Europe*, United States Government Publishing Office, Washington, 2015, Documents 177-234, pp. 527-749.
8. MacDonald, S. (1983). *Sailing into the Black Sea*, in *Surface Warfare Magazine*, vol. 8, nr. 3, pp. 2-8.
9. *România Liberă*, year XXXIII, nr. 9538, 25 June 1975, p. 5; year XXXIV, nr. 9918, 14 September 1976, p. 5.
10. *Scînteia*, year XXXVIII, nr. 8145 and 8146, 3 and 4 August 1969, pp. 1-2; nr. 9713, 6 December 1973, p. 1; year XLIV, nr. 10126, 12 March 1975, p. 5; nr. 10130, 16 March 1975, p. 4; year XLIV, nr. 10274, 2 September 1975, p. 4; nr. 10277, 5 September 1975, p. 5; nr. 10278, 6 September 1975, p. 6; year XLIV, nr. 10204, Thursday 12 June 1975, p. 1; year XLIV, nr. 10248, 2 august 1975, p. 1; nr. 10249, 3 august 1975, pp. 1-5; year XLIV, nr. 10212, 21 June 1975, p. 5; nr. 10215, 25 June 1975, p. 3; year XLIV, nr. 10274, Tuesday 2 September 1975, p. 4.; nr. 10278, 6 September 1975, p. 6; year XLIV, nr. 10277, Friday 5 September 1975, p. 5; year XLV, nr. 10593, 10 September 1976, p. 5; nr. 10596, 14 September 1976, p. 5; year XLV, nr. 10593, 10 September 1976, p. 5; year XLVII, nr. 11087 ÷ 11091, 13 ÷ 18 April 1978; year XLVII, nr. 11278, 24 November 1978, pp. 3-4; year XLVII, nr. 11277, 23 November 1978, p. 5; nr. 11.281, 28 November 1978, p. 5; year XLVII, nr. 11287, 5 December 1978, p. 4; nr. 11289, 7 December 1978, p. 6; year XLVIII, nr. 11.453, Tuesday 19 June 1979, p. 5; nr. 11.459, Tuesday 26 June 1979, p. 5; year XLVIII, nr. 11453, Tuesday 19 June 1979, p. 5; year XLVIII, nr. 11.453, Tuesday 19 June 1979, p. 5; nr. 11.459, Tuesday 26 June 1979, p. 5; year XLVI, nr. 10906, 13 September 1977, p. 3.
11. Tănase, M. (20240). *Prezența navală americană în Marea Neagră (1960-1975)*, in *Revista de Istorie Militară*, nr. 3-4 (203-204)/2024, pp. 63-78.
12. *The New York Times*, 10 December 1978.
13. *The Washington Post*, 9 December 1978.
14. Treadway, J.A. (2005). *Hard Charger!: The Story of the USS Biddle (DLG-34)*, Ed. iUniverse.
15. United States Department of State, Bureau of Public Affairs, *Seventh Semiannual Report by the President to the Commission on Security and Cooperation in Europe on the Implementation of the Helsinki Final Act*, June 1, 1979 – November 30, 1979, Special report no. 62, 1979, Washington D.C., p. 9.
16. Wats, L.L. (2012). *Ferește-mă, Doamne, de prieteni. Războiul clandestin al blocului sovietic cu România*. București: Editura RAO.
17. <https://ia600605.us.archive.org/23/items/StateDeptcable1978-131504/State%20Dept%20cable%201978-131504.pdf>, retrieved on 22 August 2025.
18. https://en.wikipedia.org/wiki/USS_Richmond_K._Turner, retrieved on 12 August 2025.
19. <https://www.navysite.de/cruisebooks/cv67-77/009.htm>, retrieved on 22 August 2025.
20. <https://www.navysite.de/dd/ddg2.htm>, retrieved on 12 August 2025.





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