ROMANIAN MILITARY THINKING

ROMANIAN MILITARY THINKING INTERNATIONAL SCIENTIFIC CONFERENCE PROCEEDINGS

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

NOVEMBER 2020
BUCHAREST

2ND EDITION

PUBLISHER
THE DEFENCE STAFF

CONFERENCE ORGANISING COMMITTEE

Chairman:
Lieutenant General Vasile TOADER

Vice-Chairmen:
Major General Teodor INCICAȘ, BEng, PhD
Major General Gheorghiță VLAD
Major General Corneliu POSTU

Members:
Major General Iulian BERDILĂ
Major General Viorel PANĂ, PhD
Rear Admiral (UH) Mihai PANAIT
Brigadier General Claudiu-Mihail SAVA
Brigadier General Ciprian MARIN
Brigadier General
Constantin NEGREA, BEng, PhD
Brigadier General Mircea GOLOGAN
Brigadier General
Nicolae MARIA-ZAMFIRESCU, BEng
Brigadier General Marian BOTEA
Brigadier General Gheorghe DIMA, PhD
Brigadier General Dorin PLEȘCAN
Brigadier General
Constantin VIZITIU, BEng, PhD
Air Flotilla General Gabriel RĂDUCANU, PhD
Captain (N) Associate Professor
Toma ALECU, BEng, PhD

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

DTP
Adelaida-Mihaela RADU

EDITORIAL OFFICE
Bucureşti, str. Izvor nr. 110, sector 5
Postal code: 050564
Tel.: +4021.319.48.80/1005320; 1005484; 1005134
E-mail: gmr@mapn.ro
Web: gmr.mapn.ro

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

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

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

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

CTEA
Printed
at Military Technical Publishing Centre
C ___/___ B ___

ROMANIAN MILITARY THINKING

INTERNATIONAL SCIENTIFIC CONFERENCE PROCEEDINGS

MILITARY STRATEGY COORDINATES UNDER THE CIRCUMSTANCES OF A SYNERGISTIC APPROACH TO RESILIENCE IN THE SECURITY FIELD

2ND EDITION

Print: ISSN 2668-7984, ISSN-L 2668-7984
Online: ISSN 2668-8115, ISSN-L 2668-7984

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

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

NOVEMBER 2020

INTERNATIONAL SCIENTIFIC COMMITTEE

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

Captain (Ret TR Navy) Assoc. Prof. Taner ALBAYRAK, PhD, PiriReis University, Istanbul, Turcia (expertise: maritime security, strategy and geopolitics at the Black Sea)

Assoc. Prof. Captain (BG Navy) Nedko DIMITROV, PhD, Dean, Bulgarian Naval Academy, Varna, Bulgaria

Dirk DUBOIS, Head of European Security and Defence College, Belgium

Prof. Jaromir MARES, PhD, Brno, Cehia

Prof. Pavel OTRISAL, PhD, Brno, Cehia

Sorin DUCARU, Director of the European Union Satellite Centre, Spain

Assoc. Prof. Iulian FOTA, PhD, National Intelligence Academy *"Mihail Viteazul"*, Romania

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

Oana POPESCU-ZAMFIR, Director, GlobalFocus Center, Romania

Scientific Researcher II Carmen Sorina RÂJNOVEANU, PhD, Director, Institute for Political Studies of Defence and Military History, Romania

William D. HATCH, PhD, Naval Postgraduate School, Monterey, SUA

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

Prof. Marius Victor ROȘCA, PhD, prorector for education, *"Carol I"* National Defence University, Romania

Prof. Daniel GHIBA, PhD, prorector for scientific research and interinstitutional relations, *"Carol I"* National Defence University, Romania

Prof. Ion PURICEL, PhD, prorector for international relations, *„Carol I"* National Defence University, Romania

Prof. Valentin DRAGOMIRESCU, PhD, prorector for lifelong learning, relations with students and career guidance, *"Carol I"* National Defence University, Romania

Prof. Ioana ENACHE, PhD, decan, Command and Staff Faculty, *"Carol I"* National Defence University, Romania

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

Prof Gheorghe MINCULETE, PhD, Command and Staff Faculty, *"Carol I"* National Defence University, Romania

Assoc. Prof. Laurențiu-Răducu POPESCU, BEng, PhD, Command and Staff Faculty, *"Carol I"* National Defence University, Romania

Assoc. Prof. Niculai-Tudorel LEHACI, PhD, Command and Staff Faculty, *"Carol I"* National Defence University, Romania

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

Assoc. Prof. Marius ȘERBESZKI, PhD, Command and Staff Faculty, *"Carol I"* National Defence University, Romania

Prof. Florin NISTOR, PhD, Command and Staff Faculty, *"Carol I"* National Defence University, Romania

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

Prof. Laurențiu GRIGORE, PhD, Command and Staff Faculty, *"Carol I"* National Defence University, Romania

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

Assoc. Prof. Cosmin OLARIU, PhD, Security and Defence Faculty, *"Carol I"* National Defence University, Romania

Prof. Dorel BUȘE, PhD, Security and Defence Faculty, *"Carol I"* National Defence University, Romania

Lect. Cristian ICHIMESCU, PhD, Security and Defence Faculty, *"Carol I"* National Defence University, Romania

Assoc. Prof. Ciprian IGNAT, PhD, Security and Defence Faculty, *"Carol I"* National Defence University, Romania

Lect. Florian BICHIR, PhD, Security and Defence Faculty, *"Carol I"* National Defence University, Romania

Assoc. Prof. Florin POPESCU, BEng, PhD, Security and Defence Faculty, *"Carol I"* National Defence University, Romania

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

Assoc. Prof. Ruxandra BULUC, PhD, Security and Defence Faculty, *"Carol I"* National Defence University, Romania

Assoc. Prof. Ciprian PRIPOAE-ȘERBĂNESCU, PhD, Security and Defence Faculty, *"Carol I"* National Defence University, Romania

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

Lect. Dan PETRESCU, PhD, Centre for Defence and Security Strategic Studies, *"Carol I"* National Defence University, Romania

Scientific Researcher II Alexandra SARCINSCHI, PhD, Centre for Defence and Security Strategic Studies, *"Carol I"* National Defence University, Romania

Scientific Researcher II
Cristina BOGZEANU, PhD, Centre for Defence and Security Strategic Studies, *“Carol I”* National Defence University, Romania

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

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

Scientific Researcher III
Marius-Titi POTÎRNICHE, PhD, Centre for Defence and Security Strategic Studies, *“Carol I”* National Defence University, Romania

Scientific Researcher III
Crăișor IONIȚĂ, PhD, Centre for Defence and Security Strategic Studies, *“Carol I”* National Defence University, Romania

Prof. Ghiță BÂRSAN, BEng, PhD, Rector, *“Nicolae Bălcescu”* Land Forces Academy, Romania

Prof. Vasile CĂRUȚAȘU, PhD, Prorector, *“Nicolae Bălcescu”* Land Forces Academy, Romania

Assoc. Prof. Ioan VIRCA, BEng, PhD, Prorector, *“Nicolae Bălcescu”* Land Forces Academy, Romania

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

Assoc. Prof. Constantin GRIGORAȘ, PhD, *“Nicolae Bălcescu”* Land Forces Academy, Romania

Assoc. Prof. Lucian ISPAS, PhD, *“Nicolae Bălcescu”* Land Forces Academy, Romania

Assoc. Prof. Aurelian RAȚIU, PhD, *“Nicolae Bălcescu”* Land Forces Academy, Romania

Lect. Ioan-Dan POPA, BEng, PhD, *“Nicolae Bălcescu”* Land Forces Academy, Romania

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

Assoc. Prof. BEng Dorel BADEA, PhD, *“Nicolae Bălcescu”* Land Forces Academy, Romania

Assoc. Prof. Alexandru BABOȘ, PhD, *“Nicolae Bălcescu”* Land Forces Academy, Romania

Assoc. Prof. Paul TUDORACHE, PhD, *“Nicolae Bălcescu”* Land Forces Academy, Romania

Prof. Mircea VLADU, PhD, *“Nicolae Bălcescu”* Land Forces Academy, Romania

Prof. Toma PLEȘANU, BEng, PhD, *“Nicolae Bălcescu”* Land Forces Academy, Romania

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

Prof. Mihai-Marcel NEAG, PhD, *“Nicolae Bălcescu”* Land Forces Academy, Romania

Prof. Dănuț MOȘTEANU, BEng, PhD, *“Nicolae Bălcescu”* Land Forces Academy, Romania

Assoc. Prof. Ștefania BUMBUC, PhD, *“Nicolae Bălcescu”* Land Forces Academy, Romania

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

Lect. Crenguța-Mihaela MACOVEI, PhD, *“Nicolae Bălcescu”* Land Forces Academy, Romania

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

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

Assoc. Prof. Cătălin POPA, PhD, *“Mircea cel Bătrân”* Naval Academy, Romania

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

Prof. Ioan BONDREA, PhD, Rector, *“Lucian Blaga”* University, Romania

Prof. Claudiu-Vasile KIFOR, PhD, Prorector, *“Lucian Blaga”* University, Romania

Prof. Lucian-Ionel CIOCA, PhD, *“Lucian Blaga”* University, Romania

Prof. Adrian CURAJ, PhD, UEFISCDI, Romania

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

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

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

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

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

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

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

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

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

CONTENTS

INTELLIGENCE AND SECURITY

MILITARY THEORY AND ART

DEFENCE RESOURCES MANAGEMENT

MILITARY STRATEGY COORDINATES UNDER THE CIRCUMSTANCES OF A SYNERGISTIC APPROACH TO RESILIENCE IN THE SECURITY FIELD

OPENING REMARKS

Lieutenant General Daniel PETRESCU

Chief of the Defence Staff

In a period marked by the pressure of professional commitments, we have managed to meet, even in this format, within the scientific debate project organised by the enthusiastic members of the Romanian Military Thinking journal staff. I begin, therefore, by thanking every participant, especially because I believe that this project will generate valuable ideas, with applicability in the field of military science. I would like to express, on behalf of the Defence Staff, the appreciation of your willingness to share the expertise you have in your fields of activity. Our expectations of the debates are related to their multidisciplinary and useful content, which can have an impact on military planning and concepts.

The chosen title – "Military Strategy Coordinates under the Circumstances of a Synergistic Approach to Resilience in the Security Field" – proposes a topical issue: defence, approached synergistically and intelligently, increases efficiency in our noble mission, that of serving national interests. It is important for the actors involved to reach a common understanding of the concept of resilience, addressed in a double key, as it is specified in the National Defence Strategy for the period 2020-2024.

The current pandemic has shown us that in order to manage a crisis situation at the national level, and not only, it is necessary to employ systemic procedures, interconnecting, in a functional manner, various elements of states, from governments, armed forces, police, government institutions to the civil society, private sector entities and, last but not least, citizens. The pandemic has not diminished the challenges of the security environment, on the contrary, it has increased the number of security questions, for which we will have to provide answers.

I appreciate that the countries in NATO's eastern flank are still facing the most complex security context that can be encountered in this generation. What we have achieved in recent years with the Allies is to build a partnership through which we establish and design the development of common capabilities, intended to meet the potential security challenges of the future. It is important that Romania builds a future together with NATO member states and that the Romanian Armed Forces actively participate in defining this future.

The development of a security culture requires an inter-institutional approach. It is necessary to understand the new types of threats, risks and vulnerabilities, which can have an impact at individual, group, national, regional or global level. There are dangers that the civil society must be aware of in order to be able to contribute, together with the competent institutions, to their identification, prevention and combating.

The Romanian Military Thinking Conference is a useful step in this direction. We are obliged not to remain passive, to inform the general public about the challenges we face, to cultivate critical thinking and to promote the security culture.

I conclude by wishing you all success during the presentations you are going to give! I am sure that your debates will lead to conclusions with applicability in the field of national defence.

PRESENTATION OF THE CONFERENCE ROUND-TABLE DEBATES

In order to provide as comprehensive as possible points of view, at different levels of expression, the conference proposed, from an organisational point of view, an academic component, focused on the presentation and publication of scientific articles, and a debate-based component, focused on a practical perspective. Both components of the conference were covered by three sections: *Intelligence and Security, Military Theory and Art, Defence Resources Management*.

The round-table debates addressed four topical issues for the Romanian Armed Forces, in particular, and for the civil society, in general, benefiting from the knowledge shared by internationally recognised experts: *Consolidation of the National Defence System Resilience at Strategic Level; STRATCOM – Fake News and Information Warfare; Economy-Military Strategy Relationship. National Defence Industry and the Armed Forces; Defence Resources Management and the Forces Mobilisation System in the 21st Century. Territorial versus Professional Troops*.

CONSOLIDATION OF THE NATIONAL DEFENCE SYSTEM RESILIENCE AT STRATEGIC LEVEL

Within the debate having the topic *Consolidation of the National Defence System at Strategic Level*, Iulian Chifu discussed the subject *Strategic Resilience from Stability and Prevention to Proactive Action and Dynamic Adaptability*, and Antonia Colibășanu, Senior Analyst for Geopolitical Futures, presented the theme *Resilience of the Alliances in the Eastern Europe Area*. Moreover, His Excellency, Sorin Ducaru, Director of the EU Satellite Centre, debated the issue *Impact of New Technologies on Resilience: Potential Vulnerabilities and Related Effects*, and Colonel Dan Colesniuc, expert in security within the Ministry of National Defence, talked about Educational Interoperability at Strategic Level. The theme proposed by Iulian Fota, Managing Director, Romanian Diplomatic Institute, was *Clarification of the Concept of Resilience at National Level.* Alexandru Grumaz, President, Centre for Security Analysis and Strategies, presented the theme *Hybrid Warfare and Resilience Strengthening in NATO Eastern Flank*, and Colonel Daniel Ghiba talked about *Continuous Adaptation to the Transformations in the Security Environment – Key to the National Defence System Consolidation*. Major General (r) Leonardo Dinu, Director, New Strategic Centre, approached the theme *Strategic Resilience in the Context of Emergent Threats to National Security*.

The moderator of the debate was Major General Iulian Berdilă, and the special guest for that round table was Mircea Geoană, NATO Deputy Secretary General.

STRATCOM – FAKE NEWS AND INFORMATION WARFARE

The subject of the debate was *STRATCOM – Fake News and Information Warfare*. There were two sections – *Strategic Communication in the Current Security Context and Fake News: Influences and Manifestations in the Allied and Regional Information Environment*. Among the participants in the first section, Andrei Țărnea, Managing Director, Department for Communication and Public Diplomacy, Ministry of Foreign Affairs, and Colonel Valentin Vasile, Deputy Chief of the Information and Public Relations Directorate, the Ministry of National Defence, can be mentioned. *"Carol I"* National Defence University was represented by Senior Lecturer Ruxandra Buluc, PhD, Professor Mihail Anton, PhD, and Lecturer Ciprian Pripoae-Șerbănescu, PhD. The second section benefited from the presence of Alina Bârgăoanu, PhD, Dean, Faculty of Communication and Public Relations – National School for Political Studies and Public Administration (SNSPA), Oana Popescu-Zamfir, Director, Global Focus, Iulia Anghel, PhD, Lecturer, Faculty of Communication Sciences, Ecological University, Bucharest, Lieutenant Colonel Constantin Bălan, Information and Public Relations Directorate / Ministry of National Defence, and Colonel Professor Adrian Lesenciuc, PhD, *"Henri Coandă"* Air Force Academy, Brașov.

The moderator of the debate was Brigadier General Constantin Spînu, and special guests were Dirk Dubois, Director ESDC – European Security and Defence College, and Colonel Peeter Tali, Deputy Director, NATO Stratcom COE.

ECONOMY – MILITARY STRATEGY RELATIONSHIP. NATIONAL DEFENCE INDUSTRY AND THE ARMED FORCES

The third round-table debate, moderated by Major General Corneliu Postu, started from the relationship between economy and military strategy, focusing on the national defence industry. Simona Moagăr-Poladian, Director, Institute for Global Economy, Romanian Academy, was the special guest, giving a presentation about *Romania's Strategic Economic Development in the Current European and Global Context*. Simona Cojocaru, State Secretary for Defence Policy, Planning and International Relations, as well as directors of important companies in the defence industry, including the Directors of ROMARM and PATROMIL, Gabriel Tuțu and Viorel Manole, participated in the debate. Viorel Manole talked about the *Advantages of a Real Partnership between National Defence Industry and National Defence System Forces*, and Niculae Iancu, President I2DS2 (Integrated Intelligence, Defence and Security Solutions), gave a presentation entitled *Towards a National Defence Research and Industry Community*. Admiral (LH) Ion-Cristian Lișman, Deputy Chief for Resources of the Naval Forces Staff, approached the theme of *Challenges for the Naval Forces in the Current Economic and Geopolitical Context*, and Grigore Filip, Managing Director, AEROSTAR Bacău, talked about the *Evolution of the Technologies Required by the Romanian Armed Forces – Determinant* *in the Aerostar Development*. *Case Study*. Chief Commissioner Lucian Ivan, Ministry of Internal Affairs, Operational Management General Directorate, approached the theme of *Resilience at the Level of National Defence Industry*, and Colonel Tiberius Tomoioagă, Scientific Deputy, Military Equipment and Technologies Research Agency, discussed about *PESCO/EDF/EDIDP Implications on Defence Capabilities*. General (r), Director, Damen Naval Romania, talked about *Naval Industry Resilience in a Global Crisis Period*.

FORCES MOBILISATION SYSTEM IN THE 21ST CENTURY. TERRITORIAL VERSUS PROFESSIONAL TROOPS

A less debated subject so far was the *Forces Mobilisation System in the 21st Century. Territorial versus Professional Troops*. Current and former chiefs of the armed forces services as well as current and former chiefs of directorates within the Defence Staff provided different points of view related to the challenges of the forces mobilisation system in the 21st century. The special guest in that case was Marius Bălu, State Secretary and Chief of Department for Parliament Liaison and Personnel Welfare, who opened the mentioned debate by providing a legal perspective. Major General Gheorghiță Vlad was the moderator of the debate.

In the round-table discussion, Professor Ion Giurcă, PhD (*"Hyperion"* University, Bucharest) provided a historical perspective of the subject – *Territorial Troops versus Professional Forces in the First Half of the 20th Century*, and Marian Zulean, University of Bucharest, approached the *Civil-Military Relations in Contemporary Romania*. Colonel Adrian Vasiliu, Deputy Chief of Personnel and Mobilisation Directorate, the Defence Staff, talked about *Territorial Defence – Challenge or Necessity*. The subject proposed by General (r) Ștefan Dănilă, Vice-President, I2DS2, and former Chief of the Defence Staff, was *An Analysis of the Forces Mobilisation System in the 21st Century. Territorial Troops versus Professional Forces*. Major General (r) Florian Răpan drew the audience attention to the theme: *Strategic Management or Strategic Planning in the Field of Defence?* Major General Viorel Pană, Chief of the Air Force Staff, presented *A SWOT Analysis: Professional Forces vs. Territorial Troops*, and Rear Admiral (UH) Mihai Panait, Chief of the Naval Forces Staff, approached *Sufficiency of the Vision of the Romanian Naval Forces Modernisation to Fully Accomplish the Assigned Missions in National and Allied Framework*. *"Nicolae Bălcescu"* Land Forces Academy from Sibiu was represented by Colonel (r) Toma Pleșanu who talked about *Generational Interoperability of the Human Resource in the Ministry of National Defence*. Lieutenant General (r) Virgil Bălăceanu, President, Romanian Reserve Officers Association, approached the theme *Complementary Character of Territorial Forces in National Defence*.

THE MAIN IDEAS PROMOTED WITHIN THE DEBATES ARE AS FOLLOWS:

- the definition of resilience needs to be clarified so that everyone can operate with the same concept;
- in Romania's Defence Strategy for the period 2020-2024 the focus is on resilience – an element of modernity, an anticipatory element, which is reflected in Romania's fundamental strategic document in a correct and ambitious manner. In fact, in Romania, it provides the foundation for a good strategic governance;
- Romania can and must play an important part in refining the dialogue related to resilience at the Alliance level as well as at the international one;
- the most important competition is the competition for ideas, for the philosophy that governs our way of organising as a society;
- building the resilience of the Western society and the defence infrastructure in Eastern Europe should be our priority in terms of individual nation, region, and transatlantic partnership;
- at the European Union level, it has been acknowledged the fact that the organisation is able to have a unitary approach, which includes all the components that define resilience at the societal level;
- resilience 1.0 entails prevention and stability, resilience 2.0 refers to proactive action and early warning, resilience 3.0 means dynamic adaptability;
- the state resilience is different from the country resilience;
- the religious vein is the *"soft"* influence, which can be adopted at the political level and can be used in influencing the potential security threats in Europe;
- STRATCOM is seen, at the Alliance level, rather as a continuous process than as a capability. This process should promote a better understanding of the function of communication, beyond the traditional approaches in the mass media;
- NATO STRATCOM final goal is related to meeting NATO policies final objectives, and, in this context, a primary desiderate is to protect and promote the Alliance key messages;
- social networking sites are not interested in providing correct information but in maximising their profit;
- our level of attention is constant, while the sources of information increase exponentially;
- the sources of disinformation are structural, not circumstantial, being related to the speed and complexity of the phenomenon, to the explosion of social media platforms and the information bombardment;
- infodemic is correlated with the actions of some hostile state and non-state actors;
- infodemic is not limited to information warfare, there is no sign of equality between the two phenomena. Infodemic is also linked to certain tendencies of people to amplify, to tell stories, to transmit to others;
- the new type of soldier: the influencer, capable of using communication in order to have effects on those insufficiently prepared to respond adequately;
- reactive response – the usual products of strategic communication are insufficient once the new ways of influencing get diversified and benefit from the even unforeseen possibilities provided by new technologies;
- the fake news-type action produces effects on the information infrastructure of the military organisation and of the state structure, discrediting the institutions and decreasing the level of trust in them;
- a high level of security culture, obtained by the democratisation of the hybrid confrontation, allows for the transformation of all citizens of the state, be they military or civilian, into agents of positive change.

CHANGING THE INTELLIGENCE COMMUNITY CENTRE OF ANALYTICAL INTEREST

Raluca-Mihaela STĂNESCU

Defence Intelligence Training Centre, Bucharest

The numerous and various challenges that have arisen in recent years in the so-called "knowledge society", where globalisation has played a key role in impacting the information environment, have led to a number of changes at theoretical, conceptual, cognitive and even behavioural level for experts activating in the intelligence field. Due to the growing dynamics of events, the value of information is now subject, more than ever, to an accelerated process of obsolescence, and the sources' level of credibility often risks to be ignored by the desire to ensure the beneficiary's fastest possible accessibility to information. As such, the knowledge-based analytical process model is more and more validated by the intelligence community, to the detriment of the information-based analytical process model used until recently.

Keywords: intelligence; analysis; knowledge; analytical model; fake news;

INTRODUCTION – THE TRANSITION TO EVIDENCE-BASED INTELLIGENCE

History will show us whether the recent reforms in intelligence services are evolving or revolutionary, but for now, the Information Community (IC) is responding to the changes imposed by the events of 11 September 2001, which overturned the entire analytical information scaffolding that existed until then. In particular, the analytical and collecting communities are trying to include in their work one of the pillars of the new legislation adopted post 9/11 – improving the exchange of information between services. As reforms occur, the collector and analyst need to adapt to new analytical rules and standards to incorporate more and more methodologies, techniques and alternatives into their analysis, under the coordination of managers and in collaboration with various national intelligence organisations. These new structures and guidelines are a real intellectual challenge, but also a bureaucratic maze for the collector and analyst, who struggle not only to *"produce"* information in a timely manner, but also to permanently improve their product, which is difficult for the intelligence professional who never has time on his side. This is why improving the mental resources of analysts is so important, and elements of understanding and sensory knowledge could propel the profession beyond the *"known analytical paradigm"* applied to complex problems, creating greater premises for the use of imagination in the IC.

Moreover, the *"infodemy"* that characterises the public information space, through intoxication with fake news, propaganda and manipulation, needs firm countermeasures, calibrated even on adapted and reinvented analytical models, designed to ensure public access to valuable and real information Voicu, 2020).

In this volatile and unpredictable context, in addition to cultivating individual discernment, creators of informational reports use more than contextual data and information. They use sets of evidence, data collections and structured information relevant to the problem to be analysed – in other words, contextualised to each specific problem. Evidence reveals alternative explanations through induced inferences, based on mental patterns about what will happen or what has already happened in the past[1].

[1] Reasoning about past events remains easier than reasoning about the future. In the first case, the evidence may be contradictory, misleading and subject to several interpretations. However, it tends to be more complete and better organised (or at least discoverable). Looking to the future, we can say that much of the evidence does not yet exist. The events described by the ominous information may not have occurred. In addition, the information that should become evidence usually remains incomplete.

While inferences are usually uncertain, they justify beliefs about phenomena, processes, situations, and people. Their justification (or theories/hypotheses) is relevant to their accuracy, but does not guarantee the *"absolute truth"*. Rather, as Peter Kosso (2006, p. 4) observed, justification of beliefs means *"compliance with the standards of evidence and reason [to] indicate the [probability] of accuracy"*. This is where informational sensemaking comes into play, a superior component of analytical thinking, which is the type of predictive intuitive-heuristic thinking developed by the analyst (Stănescu, 2016, p. 94) in an attempt to establish *"a correlation between being more justified and being true"* (Ibid.).

For example, during a recent exercise, a team of analysts came to an inferential conclusion about a likely explanation for the phenomenon examined. Participants were presented with a set of previously established alternative conclusions and a set of relevant presumptive evidence and were asked to assess which conclusions were justified and true. After reaching an initial conclusion, they were asked to consider an alternative conclusion annulling the truthfulness of the first one. In doing so, they found that while the initial conclusion seemed more accurate, the second was in fact *"true"*. This was partly because they made biased assumptions about the evidence they used, to justify their findings. As Kosso (Ibid., p. 4) noted, *"better justification increases the likelihood of accuracy. But it is very possible that a well-justified belief is false"*.

This stage of work subsequently led to a more critical assessment of the evidence, many of which proved to be false. Participants found that *"justification comes gradually, but the truth is not"* (Ibid., p. 5). It is therefore arguable whether a greater evidentiary justification indicates the likelihood of a more accurate correlation with the truth. As Kosso pointed out, even with good justification, there is no certainty in establishing the truth. Therefore, according to the same author, *"it is the task of systematic disciplines ... to carefully refine the content of the justification, the evidence and the set of theoretical beliefs, to bring the justification in an increasingly close correlation with the truth"* (Ibid.).

If information is to *"speak truth to power"*[2], it must first be ensured that the message conveyed is solid and critically justified.

The realisation of the awareness process takes place gradually and serves the fulfilment of several objectives, including the description of facts, the explanation of phenomena, the interpretation of events and actions and the estimation of the

[2] The phrase *"to speak truth to power"* was originally attributed to Sherman Kent. Subsequent research has invalidated this hypothesis. Regardless of the author, the semantic essence remains the same, and it is an urge for the specialists of the Information Community to correctly inform the decision-makers.

probability and impact of future actions of an enemy. As intelligence professionals move from describing events to explaining patterns of behaviour and understanding the underlying factors and intentions, there is a growing need to justify their beliefs about the problem under analysis.

However, as intelligence experts attempt to apply more rigorous scrutiny at this stage, they find that the level of ambiguity increases (Moore, 2011). In addition, analysts who apply conscious thinking are expected to be more often mistaken in the predictive stage than in the descriptive stage. This is partly due to an interesting reality characterised by Taleb: *"to predict the future we must already know the future"* (2007, p. 173). What Taleb claims is that you must have already visualised the future in order to estimate it.

Kosso (2006, p. 5), referring to epistemology, argues the following: *"[The] knowledge claims are more ambitious in that they stray further from what is immediately observed… The theoretical descriptions are based on observation and evidence… But it is important to note that the observations themselves are based on theory. Scientific evidence, after all, is neither haphazard nor uninterpreted, and some prior conceptual understanding of nature will inform decisions about what to observe, which observations are credible, what the observation means, and how what is observed is causally (and hence intentionally) linked to what is not observed. Theory is necessary to turn mindless sensations into meaningful evidence"*.

While Kosso uses a scientific language, his argument also applies to Manjoo's *"post-factual"* world, where information often tries to make sense[3]. The information is created, finally, by observing the phenomena, mediated by sensors. Moreover, the evidence in the field of information, although it may seem *"accidental"*, is the result of systematic search, collection and interpretation.

The past tells practitioners what information to look for in the future. This can be a trap when the indicators are no longer valid. As Baruch Fischoff (1982, p. 338) suggests, *"the search for wisdom in historical events presupposes an act of faith – a belief in the existence of recurring patterns waiting to be discovered"*.

However, although there may be general patterns, *"the past is never repeated in detail"* (Ibid., p. 336). In other words, there may be indicators that suggest that a future event, similar to the past, is possible, probable, or even reasonable. Based on such reasoning, we might anticipate, for example, that foreign terrorists will attack the United States of America again, targeting an important building, such as the

[3] By *"post-factum"*, Manjoo refers to the tendency to ignore evidence, thus favoring preconceived conclusions. An example of this is the refusal of some parents to vaccinate their children, which is due to pseudo-scientific conclusions. Within IC, this trend is manifested when intelligence specialists allow their analytical efforts to be guided by certain predetermined conclusions, despite the evidence that seeks to identify new hypotheses.

World Trade Center[4], or a large-scale event (Mylroie, 1995). Undoubtedly, this was not a prediction of the 9/11 attacks, when Al Qaeda terrorists struck the Twin Towers and the Pentagon aboard planes over which they took control and crashed into buildings[5]. Finally, the problem-solving intelligence experts rely heavily on theories that, if not proven, are in fact unexamined hypotheses. If using the past to gain wisdom about what the future holds is not feasible, why not study the past to avoid certain mistakes? Another conclusion that emerges and has been largely evaluated by specialists is that the focus on misfortunes *"disproportionately increases their perceived frequency"* (Fischoff, p. 339; Tversky et al., 2003, pp. 207-232).

Another challenge that must be considered when analysing the past from the perspective of what should be avoided is the problem misunderstanding. While understanding may be possible, or even easier when dealing with normal issues, when it comes to wicked issues, such an understanding is at best evasive and depends on the methods chosen to solve them; in other words, regrettably incomplete.

With the intent of improving the creation of evidence-based information, recent US legislation that *"reshapes"* intelligence services goes so far as to require *"alternative analysis"* (US Congress, 2004, p. 330). IC, through its schools, interprets this in the sense that several hypotheses must be considered. The relevant legislation mentions *"the red team: a means by which another group of intelligence professionals launches alternative explanations for a problem that is being analysed"* (Ibid.). The legislation does not address the issue of criteria for achieving awareness in the case of analysing normal problems and especially wicked problems that arise as a result of conflicting intentions. If, for example, it is estimated that a particular country will develop both long-range missiles and a nuclear capability, so that, finally, we can analyse a possible combination of the two capabilities, we must take into account the context of the political and technological environment of the target country, what is a long-range missile, what is a nuclear weapon, what is a weapon of mass destruction and, last but not least, we must have sufficient availability to analyse a potential combination of all these threat elements. Political decision-makers can disapprove the actions of the target country, making their leaders more virulent. Thus, intelligence services and policy makers create the future – or, at least, a version of it. If all these aspects are analysed unprofessionally or superficially, there is a risk of unintended and dangerous implications.

[4] On February 26, 1993, a trap truck placed by Islamic terrorists exploded under one of the World Trade Center buildings and apparently aimed to demolish both towers (Mylroie, 1995).

[5] However, the attacks had been anticipated. According to comments made by Schwartz and Randall, *Many people did predict the 9/11 attacks [2001]... Despite predictions, many US officials in the Clinton and Bush administrations focused on other elements, while the inevitable became imminent."* (Schwartz and Randall, 2007, p. 94).

The final result is a mixture of hypotheses ready to be challenged point by point, although the tendency of information professionals is to create permanent uncertainties, which can prevent such a situation. If, on the contrary, the assessment is wrong, and the assessed nuclear capability for weapons production is in fact intended to provide an alternative to the nation's dependence on a declining supply of increasingly expensive oil supplies, and the missiles support a space programme designed to orbit telecommunications satellites that can meet the needs of the country and their neighbours, as well as to provide additional revenue to the state budget, then analysts and decision makers will have inappropriate extrapolated models, resulting from an incomprehensible present. In a tense bilateral or multilateral environment, rhetoric and actions can precipitate events so as to create a future in line with those patterned conclusions, causing the target country to produce weapons. In the end, each side blames the other nation's government for having "caused" the crisis.

There are several reasons for such faulty causal networks. Honest evidentiary considerations require a degree of agnosticism about the justification of theories. Evidence-based knowledge is not absolute; justified evidence changes theories and not the other way around. In other words, existing or accepted theories need to change only when interpretations of evidence lead to coherent alternative inferential conclusions. What should not happen is to reinterpret the evidence to support the prevailing pre-existing theory, as is the case in the example above. However, this is exactly what happens most often. People are often unwilling to give up on their precious positions.

This is partly due to the fact that, as they reflect on the evidence, they do not become involved. In other words, their opinions are influenced by different worldviews or cognitive approaches, especially selective perception and selective exposure. These elements combine to guide the way people perceive problems, the phenomena that make them up, and how they strive to make sense of them[6]. These influences or theoretical frameworks shape the patterns that people use to interpret new phenomena. The advantage is that these patterns make people smart and transform their thinking quickly, gradually evolving from patterns of behaviour to survival mechanisms (Gigerenzer, 1999). However, this advantage depends on the recurrence of the phenomena. In order to function successfully, an intuitive framework of understanding presupposes the appearance of at least

[6] More information on *"heuristics"* and the mental patterns people use in their analytical reasoning is presented in papers such as those of Kahneman, Slovic, Tversky, Gilovich, Griffin.

a similar situation, a condition that is often missing in the analytical environment of intelligence. In an information-rich environment, based on technical collection, information specialists can select inappropriate models to use in understanding new phenomena. In intelligence work, if such models conspire to affect the search and selection of evidence used by analysts, selective perception and selective exposure do nothing but facilitate the occurrence of error and failure. Evidence always requires context and, as the example above illustrates, multiple meaningful explanatory contexts can coexist simultaneously. In intelligence, *"evidence is [particularly] rarely self-sufficient in information or credibility"* (Kosso, 2006, p. 8). In addition, the nature of the evidence itself, when viewed outside the political and social context, contributes to the failure to properly explore the issues.

In other words, unless the correct context is known, the evidence – if its constitutive information can even reach that threshold – is subject to many different interpretations. Outside the context, the person evaluating the evidence can select the correct interpretation. Multiple contexts confuse the situation, as different contexts often lead to alternative conclusions, as illustrated in the missile development scenario described above. Finally, the political context of the decision-maker may distort the actual context transmitted through the information.

What happens in the contextual consideration of evidence is a process of epistemological justification and, as Kosso (Ibid., p. 4) observes, the *"key concern is to distinguish knowledge, on the one hand, from mere belief, opinion, dogma, and wishful thinking, on the other"*. In relation to the information, knowledge depends on the contextual justification of the evidence and, as mentioned earlier, the *"business of epistemology is to show that there is a correlation between being more justified and being more likely to be true"* (Ibid.). Despite their inevitably greater inaccuracy, the predictions seem to arouse more interest from the beneficiaries than the explanations. In biology, to be useful, predictive assumptions require adaptation to valid background information. Does this also apply in intelligence? As illustrated in two national information estimates (NIEs) dealing with weapons of mass destruction (WMD) and which were later found to be wrong, incorrect predictions certainly drew special attention. In these cases, incorrect predictions probably resulted, in part, from analysts' lack of time to develop them. In the first case, the estimate of whether or not the Soviets would place strategic nuclear missiles in Cuba in 1962 was written within a week[7]. In the case of Saddam Hussein's WMD programmes, the preparation time was three weeks. Such short periods of time would seem to prevent the collection of new information and data that would become relevant to those issues (i.e. analysed as evidence), preventing the full exploration of alternative perspectives[8].

Lack of time characterises a context for achieving information sensemaking. This context in which information experts work and the constraints imposed on them facilitate their successes, but also their failures. As the examples above prove, information producers are often under pressure and fail to take into account massive amounts of data and information in a short time. The same professionals need to organise data and information into evidence, in order to understand and then explain to decision-makers and beneficiaries the complex issues associated with it. Finally, current and past intelligence practice focuses on prediction, rather than explanation, as the ultimate goal. This was not without criticism. Willmoore Kendall, in the revised edition of the book written by Kent in 1949 for World Politics, criticised Kent's *"compulsive preoccupation with prediction"* (Kendall, 1949, p. 549). Given the experience of Kent and others during World War II, it is not surprising that the desire to prevent another Pearl Harbor dominated their practices; such a desire would naturally have led to an activity organised around the creation of predictive knowledge that prevents surprise[9].

"NORMAL INTELLIGENCE" VS *"STRUCTURED INTELLIGENCE"*

The process described above can be considered *"normal intelligence"*. As Thomas Kuhn conceived it, the *"normal"* refers to *"the relatively routine work… within a paradigm, slowly accumulating detail in accord with established broad theory, not actually challenging or attempting to test the underlying assumptions of that theory"* (Normal Science). Thus, we can see that *"normal intelligence"* is an activity of expanding the knowledge in which most information professionals are engaged and which gradually increases the knowledge about the targeted phenomena (Kuhn, 1962, pp. 10-42). Professionals think and work within a model or *"paradigm"* of reality forged during World War II and consolidated throughout the ensuing Cold War.

[7] As it is well known, this is a hindsight analysis. Sherman Kent stated in 1964 that, retrospectively, the authors had sufficient time to assess the evidence. See Kent, 1964, pp. 1-18. Originally classified, this document has been declassified and republished in *Intelligence Studies*, (1992, pp. 111-119). Kent carefully analyses the reasons why the analysts' assessment was wrong and not revised. These reasons include the previous course of action of the Soviet foreign policy directorates, which were presumed to be resumed in the future. Thus, no offensive missiles were to be placed in Cuba.

[8] The Senate report on Iraqi WMD noted that alternative scenarios had not been considered, although the same cannot be said of the aluminum pipeline that was allegedly intended for the production of centrifuges and rockets. Under such circumstance, it seems that the results were dictated by collective thinking. See US Senate Report on Information Assessments Prior to the Outbreak of the Iraq War, (2004, pp.18-21).

[9] Most likely, in the case of the WMD, the *"worst case scenario"* was taken into account, which partly explains the views on the nuclear programme developed by Iraq and the conclusions of the 2002 evaluation. The same cannot be said of the *"failures of the imagination"* due to which the attacks of 11 September 2001 could not be anticipated.

Past successes, as perceived at the time, contribute greatly to the repeated use of invalid art. The paradigm involves opponents at the level of actors, whether state or non-state, who have mutually destructive capabilities. In this context, *“normal information”* becomes *“information”*, as the *“normal science”* stated by Thomas Kuhn represents *“science”*.

In both areas, newly acquired knowledge is gradually being added to an increasingly defined paradigm; new knowledge does not easily redefine the paradigm. Even the extraordinary and truly new aspects are considered exclusively from the perspective of the unknown. Normal science or ordinary information does not seek to significantly revise the paradigm in which new phenomena are known and understood. This must also be seen in the light of the way in which newly hired intelligence staff work and take over existing databases. A common practice involves reviewing previous reports, with the tendency for new reports to remain within the conceptual limits of what has been previously developed. Knowledge grows only gradually. Intelligence analysts working in the mundane information paradigm try to describe, explain, or predict phenomena consistently. In this case, the term refers to another concept developed by Kuhn: A common framework for understanding phenomena is sought or assumed. New knowledge is understood in the context of the dominant paradigm.

For example, normal information from the second half of the twentieth century understood events according to the missions and objectives of American adversaries, mainly the former Soviet Union and to a lesser extent, China. World affairs were understood in the context of the hegemonic competition of the opposing USA states. Normal paradigms prevail until previously unobserved and unobservable discrepancies create sufficient inconsistencies in explaining and understanding the phenomena so as to cause errors that cannot be ignored. For Kuhn, this means a necessary change in scientists’ perceptions of the realities of science. Kuhn illustrates this with an example of the transition from Ptolemaic to Copernican astronomy. Before they appeared, the sun and the moon were planets, but the earth was not. After that, the Earth was a planet, like Mars and Jupiter; the sun was a star, and the moon was a new body type, a satellite. Changes of this kind were not just corrections of the individual mistakes included in the Ptolemaic system. They involved not only changes in the laws of nature, but also changes in the criteria by which some terms of these laws were attributed to nature. In addition, these criteria were partly dependent on the theory that validated them (Kuhn, 1970, Conant, 2000, p. 15).

In physics, the phenomena themselves do not change (although recently observed phenomena might make them look like this). In the cultural environment of human interaction, new perceptions of reality may be sufficient to force a reconsideration of the old. In social scientific terms, a new paradigm not only explains the new, but does better in explaining the old. Moreover, even the language previously used to describe a phenomenon is inappropriate because, as Kuhn (Ibid., p. 15) remarks, *“scientific development cannot be quite cumulative. One cannot get from the old to the new simply by an addition to what was already known”*. Failure to analyse discrepancies causes potential information creators to maintain a misunderstanding of phenomena, even if the phenomena change. This major discrepancy leads to either errors or information failures. According to Kent’s paradigm, information errors derive from *“factual inaccuracies in analysis resulting from poor or missing data”* (Johnston, 2005, p. 6).

On the contrary, as noted, information failures refer to *“systemic organisational surprise resulting from incorrect, missing, discarded, or inadequate hypotheses”* (Ibid., p. 6). The previous concept was that if more data were available or better understood, errors could be prevented. In the latter, intelligence practitioners or their political clients misunderstood both the issue and its context. The existence of certain information errors does not necessarily indicate a changed paradigm. However, repeated information errors do. As in the case of science, small errors in the proper characterisation of phenomena lead to the emergence of *“corrective constants”*. It is possible that the person giving the information made a mistake in perception or interpretation. However, left unchecked, errors eventually combine to cause systemic failures.

Information practitioners and policy makers can repeatedly draw erroneous conclusions from the misinterpretation of meaning, defined by Rob Johnston as *“systemic organisational surprise”* (Ibid., p. 6), resulting from a mixture of practitioners’ gaps and the disinterest of policy makers. A more appropriate interpretation would be that the failure of information stems from shortcomings on the part of both policy makers and information professionals in recognising a fundamental and revolutionary change in the information context.

The state-as-adversary paradigm for information creation is obsolete. Two decades now separate the interpretable information context from that of the Cold War: adversaries and problems are now strikingly different[10]. The power of the Soviet Union declined dramatically after 1990, while China rose. But more importantly, in an informative context, new non-state-based phenomena have emerged: non-state actors have added new challenges, threatening traditional state structures. Emerging phenomena, such as epidemics, pandemics and climate change, have imposed new complexities. The anomalies created as a result of these new phenomena illustrate how and why normal information is no longer adequate: it can no longer characterise these phenomena in terms of threat and strategic information opportunities. The *"normal"* means of explaining the error are also inadequate. As evidenced by the various reports of the US Congress and the independent committees, the information no longer adequately describes, explains or predicts the phenomena that beneficiaries need to understand. Thus, the change in information needs to be profound and revolutionary.

CHANGING THE CENTRE OF ANALYTICAL INTEREST

Revolutions in military science, politics and military affairs are taking place because crises reveal the inadequacy of the current dominant paradigm. As Kuhn (2000, p. 92) also pointed out, an existing paradigm can *"cease to function adequately in the exploration of an aspect of nature to which the paradigm itself [has] previously led the way"*. Kuhn further argues that science is not evolving smoothly. Rather, periodic revolutions change the way phenomena are perceived and understood (Ibid. pp. 92-110). Crises anticipate such changes in the centre of analytical interest. Similarly, the serious (official) failures of the intelligence community in predicting the 9/11 attacks and Saddam Hussein's WMD programmes (both in 1990 and before the 2003 invasion of Iraq) are examples of crises that have generated a systemic reform[11].

If we analyse these failures through their official evaluations, we find the recurring appearance of certain terms: mentalities, politicisation and faulty analysis. During the same period, there are repeated attempts to impose methods of *"[social] scientific study…to analysis of complex ongoing situations and estimates of likely future events"* (Davis, 1999, ch. XV). What is missing is any systematic approach in the intelligence community. As specialist and observer Jack Davis remarked a decade ago, there are no corporate standards for how information is created, including the methods used (Ibid., ch. XXV). Although sound practice does not validate the correctness of information assessments, its absence, by definition, leads to erroneous conclusions. Contributing to this scenario is the fact that, as Aris Pappas and James Simon (2002) observed, *"[potential] opponents [are] often… driven by emotional agendas that [make] them unpredictable"*. While effective practice may not lead to solid estimates from ambiguous evidence, it would alert regular practitioners to the prospect that the actions of the same adversaries are unpredictable or, at best, only partially predictable for certain behaviours. In short, intelligence experts around the world operate in an environment similar to a booming Kuhnian revolution: the epistemology of normal intelligence is insufficient and new knowledge is needed. Recent failures highlight the need for change, as does the grey area of workforce that creates information sensitivity – new people facing new and emerging problems should feel comfortable when they identify new ways to systematise their work. Changing data and contexts can cause real storms in the minds of ordinary analysts to operate with normal information, and it could be concluded that, for practitioners accustomed to operating with normal information, a real Kuhnian-style revolution is underway.

However, a clarification needs to be made: not all information practices of *"the old school"* are worthless at present. Several significant opponents at the state level remain threats to the security of the American nation, although they are also challenged by the new non-state actors and the problems that populate the new information paradigm. Moreover, in many circumstances and in dealing with certain problems, the tacit expertise of professionals with long experience in the work of intelligence services is adequately exploited to identify the *"hidden"* meanings. These *"old hands"* possess both current knowledge and a highly evolved set of skills. Years of creative and critical thinking prove that they know how to look at issues from a variety of perspectives and have the wisdom of a deep context. As a result, it is no coincidence that in the relatively recent (2008) book, written by Roger George and James Bruce, *Analyzing Intelligence*, very experienced specialists from the intelligence services contributed. First of all, it must be said that challenges are knowledge-generating, and the expertise gained from challenges becomes valuable and necessary; secondly, it is up to each intelligence service to develop

[10] It should be noted that traditional opponents of the Cold War continue to pose threats. We can also say that emerging threats simply add to traditional ones. The dangers of the 21stcentury are complex, a major danger being their complexity.

[11] The argument that these were crises that led to a complete reset is based on the fact that, over time, it has been observed that the intelligence specialists have been as shocked by the inaccuracy of their estimates as the decision makers. In the case of the 2000 estimates of WMD held by Iraq, the CIA underestimated their level, leading to the idea that the 2002 overestimation was a compensation for the error previously made. While acknowledging the minimisation of the danger in the initial reports, the CIA rejects the idea that the 2002 estimates exaggerated the situation on the ground in order to correct the errors produced. See the press release of the Central Intelligence Agency, *"Iraq's WMD Programs: Culling Hard Facts from Soft Myths"*.

and maintain the cognitive and organisational flexibility that human resources entail with such thinking. Indeed, part of successful and revolutionary intelligence work involves gathering new meanings from old patterns that have remained hidden from those who have stopped making sense. One challenge is that *"fresh"* eyes lack knowledge of potentially relevant patterns, while *"old"* eyes cannot see things as new. Each lacks the power of the other. The experience gained by newer professionals engaging in the traditional practice of *"analysis"* affects their once fresh views even when they begin to gain relevant and necessary experience. One solution could be to adopt a core competency model (including here curiosity, perseverance and pattern recognition) based on job descriptions and mission specifications of the existing intelligence services.

A first necessary step in a process of fundamental change of the intelligence activity is the in-depth analysis of what they do, they must do and how the information professionals act. Basically, intelligence practitioners create knowledge to support their beneficiaries. In other words, intelligence practitioners are supposed to be contributors to government plans and policies at various levels where they have the opportunity to share broad strategic perspectives with national leaders, as well as to ensure that military personnel deployed in theatres of operations have access to levers for technical collection and organisation of tactical data. Last but not least, it must be remembered that this Intelligence Knowledge, together with Activity and Organisation, represents only a key component in a strategic, operational and tactical intelligence trinomial (Moore, 2005)[12]. Undoubtedly, the Activity and the Organisation also need to be reshaped, but what is absolutely fascinating in the analytical process is the Intelligence Knowledge and how it is created – in short, the sensemaking.

CURRENT ANALYTICAL MODELS

The *"information-centric"* model proved to be just as different from the *"analysis-centric"* (knowledge-based) model largely used in the United States. The information-centric model places both real and abstract value on information, not knowledge, as the main currency of information activity – having profound effects.

[12] In his work *Strategic Intelligence*, Kent identified and stated three concepts that define strategic-level information: Knowledge or what is produced and disseminated; The Activity or the way in which knowledge is produced and disseminated; and The Organisation or the way in which people are grouped to produce and disseminate that knowledge. Moore and Krizan, in the work *Core Competencies*, claimed that this approach belonged to them, and they resumed the concept with David T. Moore in the work *Evaluating Intelligence: A Competency-Based Approach*, International Journal of Intelligence and Counter Intelligence, vol. 18, no. 2, 2005.

The book by Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, now in its 7th edition, is rightly recommended as a mandatory reading for those beginning their careers in the intelligence field. This paper defines, succinctly and practically, an intelligence process that places analysis in a key position for communicating the results of information activity in the political narrative presented to decision-makers. At the strategic level, analytical products such as the President's Daily Brief or National Intelligence Estimates (NIEs) are analytical products that address the priority security issues of the United States – a kind of comprehensive picture of the latest developments in the areas of interest. At the operational level, products such as Dynamic Threat Assessments and Military Capability Studies inform military leaders about the complexities of the environment in which they may be required to engage the armed forces.

In both cases, the analysis plays a central role as the main provider of knowledge to intelligence services in the policy-making process. Decision-makers consume a constant diet of analysis and provide guidance on the direction of further information. This process can be called *"analysis-centric"* in order to compare it with how much of the world conceptualises and uses information. The analysis-centric model is usually defined as an *"intelligence cycle"* or *"intelligence process"* that characterises the interaction of functionality within intelligence services, including planning and targeting, dissemination, analysis, production, processing, and operation, with researchers such as Lowenthal that adds consumption and evaluation as distinctly identifiable additional functions.

Intelligence services provide guidance only when policy makers consider that the issues of national security interest identified can only be addressed through the substantial analytical expertise of intelligence services; these policy guidelines often appear in the form of priorities for the use of intelligence resources.

While the development of knowledge is important, the goal is to develop predictive knowledge that allows decision-makers to anticipate events, thus gaining a competitive benefit. Analysts are trained and specialised in "data mining", building complex arguments, overcoming and eliminating inherent, often subconscious biases, and assigning confidence levels to their own assessments. Analysts are also trained to articulate what information is needed in the information environment to progress from common knowledge to predictive knowledge.

Each unique intelligence discipline, HUMINT, SIGINT, IMINT and so on, has a defined collection methodology, designed to focus on the empirical objectivity of information and its effective transmission to analysts who have all the sources, in a way that allows the perfect integration of their role in the development of knowledge.

Each report resulting from the multi-INT collection requires evaluation by an analysis specialist who, in turn, informs the collector whether the information was timely and relevant for promoting the analytical report. In particular, in the case of HUMINT, analysts themselves become *"independent"* and objective intelligence consumers. This method of using analysis to assign value to the employment of collection activities is in stark contrast to the intelligence-centric model.

The intelligence-centric analysis model presents the collection of information, and not its analysis, as a primary and sustained function of the intelligence process. The effects of this type of analytical model have an impact on the definition of where the abstract value resides, how resources are used, and how expectations will be used to support information decision-making.

Knowledge development, insofar as it exists, lies in the individuals who produce or process the reports, and not as a distinct institutional mechanism.

In the intelligence-centric model, individuals, not institutions, have absolute power. This phenomenon makes it difficult to monitor or evaluate the efficiency of intelligence services by the state, and the knowledge acquired by the agencies to survive the changes that take place at the level of political leadership. Because evaluations are invariably related to individuals in leadership positions and the personal interpretation of what information means, any criticism of evaluations is personal, rather than a test of an organisation's reasoning that invariably becomes a direct challenge to authority. Because they do not have a framework in which to present contradictory assessments, decision-makers are somehow forced to continue to rely almost blindly on intelligence specialists.

The two analysis models presented are undoubtedly useful and have proven their effectiveness over time. Some would say that the intelligence-centric model would be more successfully applied to tactical and operational intelligence, while for strategic-level intelligence, the knowledge-centric model is more recommended. A clear conclusion in this regard could only be drawn from the validation, accreditation and long-term use of the two models on the aforementioned intelligence dimensions.

CONCLUSIONS

Under the circumstances of the inability to assimilate the complexity of reality or to detect in the multitude of fake news existing in the media, individuals resort to the construction of simplified mental models of the objective world, to which they superimpose the information received later, without always having a compatibility between informational input and one's own pattern of thinking.

For the current intelligence analyst, all these challenges can cause cognitive errors, with a direct impact on the information products developed.

The psychological, cultural or religious limitations that can influence both the analyst and, implicitly, the finished product developed by him, must be mitigated by applying viable analytical methods, suitable for the current security environment and usable as functional tools, based on which to develop information designed to meet the customers' needs.

Whether we are talking about analytical models based on information or knowledge, or we are talking about sensemaking, the methods chosen by analysts and, implicitly, by the intelligence community must provide them with a means of disambiguating the mysteries and difficult puzzles they have to cope with daily. Even in current practice, analysts use complex approaches when they cannot rely on a single method of acquiring meaning. While the results of different methods may be convergent, reinforcing a special understanding of a phenomenon, they may also be divergent and produce different interpretations. It is up to the intelligence practitioners to resolve all these differences and strive to make sense out of them.

For example, intelligence experts, who engage in a *"multiframe"* sensory approach, analyse and evaluate issues from several perspectives created at the confluence of action and process-focused views, or individual views versus collective views.

Whatever the methods approached, the Intelligence Community must function as a unique system capable of creating a unified picture of events and problems, based on multi-source information.

BIBLIOGRAPHY:

1. Davis, J. (2007). *Introduction – Improving Intelligence Analysis at CIA: Dick Heuer's Contribution to Intelligence Analysis, in Heuer, R.J. Jr., (1999). Psychology of Intelligence Analysis*. Washington, D.C.: Center for the Study of Intelligence, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/art3.html, retrieved on 15 September 2020.

2. Dudley, C.A. (2018). *Information-Centric Intelligence: The Struggle in Defining National Security Issues*. International Journal of Intelligence and Counter Intelligence.
3. Kosso, P. (2006). *Introduction: The Epistemology of Archaeology*, in Fagan, G.G., *Archaeological Fantasies: How Pseudoarchaeology Misrepresents the Past and Misleads the Public*. London, UK: Routledge.
4. Fischhoff, B. (1982). *For Those Condemned to Study the Past: Heuristics and Biases in Hindsight*. Carnegie Mellon University.
5. George, R.Z., Bruce, J.B. (2008). *Analyzing Intelligence: Origins, Obstacles, and Innovations*. Washington, DC: Georgetown University Press.
6. Gilovich, Th., Griffin, D., Kahneman, D. (2002). *Heuristics and Biases*, Cambridge, UK: Cambridge University Press.
7. Gigerenzer, G. (1999). *Simple Heuristics that Make Us Smart*. Oxford, UK: Oxford University Press.
8. Johnston, R. (2005). *Analytic Culture in the US Intelligence Community – An Ethnographic Study*. Washington DC: The Center for the Study of Intelligence.
9. Kahneman, D., Slovic, P., Tversky, A. (1982). *Judgment Under Uncertainty: Heuristics and Biases*. Cambridge, UK: Cambridge University Press.
10. Kendall, W. (1949). *The Function of Intelligence*. Cambridge University Press.
11. Kent, S. (1964). *A Crucial Estimate Relived*. Intelligence Studies, vol. 8, no. 2.
12. Kuhn, Th. (1962). *The Structure of Scientific Revolutions*. Chicago, IL: University of Chicago Press.
13. Kuhn, Th. (1970-1993). *The Road Since Structure: Philosophical Essays*.
14. Moore, D.T. (2005). *Evaluating Intelligence: A Competency-Based Approach*. International Journal of Intelligence and Counter Intelligence, vol. 18, no. 2.
15. Idem (2011). *Sensemaking – A Structure for an Intelligence Revolution*. Washington, DC: National Defense Intelligence College.
16. Mylroie, L. (1995). *Who is Ramzi Yousef? And Why It Matters*. The National Interest, http://www.fas. org/irp/world/iraq/956-tni.htm, retrieved on 15 September 2020.
17. Pappas A.A., Simon, J.M. Jr. (2002). *The Intelligence Community: 2001-2015: Daunting Challenges, Hard Decisions*. Intelligence Studies, vol. 46, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol46no1/article05.html, retrieved on 17 September 2020.
18. Schwartz P., Randall D., *Ahead of the Curve: Anticipating Strategic Surprise*, in Francis Fukuyama (eds.), Blindside: How to Anticipate Forcing Events and Wild Cards in Global Politics, New York: Basic Books, 2007.
19. Stanger-Hall, K. et al. (2005). *Accommodation or Prediction? Letter in Response to Peter Lipton, Testing Hypotheses: Prediction and Prejudice*. Science, vol. 308, no. 5727.
20. Stănescu, R. (2016). *Conştientizarea – componentă superioară a gândirii analitice*. *Infosfera* Journal, no. 1.

21. Taleb, N.N. (2007). *The Black Swan: The Impact of the Highly Improbable*. New York, NY: Random House.
22. Voicu, M. (2020). *Luptele nu se mai dau pentru teritoriu, ci pentru mințile oamenilor, cu o miză uriașă pentru democrație*, 2 September 2020, http://presamil.ro/marian-voicu-jurnalist-luptele-nu-se-mai-dau-pentru-teritoriu-ci-pentru-mintile-oamenilor-cu-o-miza-uriasa-pentru-democratie/, retrieved on 15 September 2020.
23. CIA Press release, *“Iraq’s WMD Programs: Culling Hard Facts from Soft Myths”*, 28 November 2003, https://www.cia.gov/news-information/press-releases-statements/press-release-archive-2003/pr11282003.html, retrieved on 17 September 2020.
24. US Congress, *Intelligence Reform and Terrorism Prevention Act (IRTPA)*, 2004, retrieved on 17 September 2020.
25. Wikipedia, *Normal Science*, http://en.wikipedia.org/wiki/Normal_ science, retrieved on 17 September 2020.

THE ROLE OF STRATEGIC COMMUNICATION IN CONTEMPORARY CONFLICT

Captain Antonia Teodora MARIȘ, PhD Student

"Carol I" National Defence University, Bucharest

The present material aims to provide a conceptual delimitation of what contemporary conflict means and at the same time to highlight the role of strategic communication in the conflicts specific to the 21st century. This new type of conflicts has strategic communication as the centre of gravity, through the methods of influencing power. The present material will include examples of how the Russian Federation manifests its power using strategic communication.

The realities of the current century emphasises new security challenges: among them, online communication is becoming more and more important, shaping a world where facts as such do not matter the most – what matters is the way they are perceived and understood.

Keywords: contemporary conflict; strategic communication; power of influence; disinformation; narrative strategy;

INTRODUCTION

In a complex and constantly changing security environment, strategic communication, when used appropriately and based on narrative strategies adapted to the cultural characteristics of the target audience, can be the most effective solution for meeting internal and external objectives of a state actor.

The implementation of the concept of strategic communication and the understanding of the role that this process plays in the 21st century derives from the current challenges to national security that include both conventional and unconventional threats specific to contemporary conflict. The influence exerted by state and non-state actors is an additional pressure in the information sphere, with the potential to change the perception of certain target audience segments, to hinder or stop the decision-making process or to discredit actions and initiatives.

In this situation, the process of strategic communication which involves, among other things, promoting national objectives, strengthening national values, combating misinformation, timely informing the population, counteracting hostile propaganda, becomes an element of great importance in contemporary conflict.

CONTEMPORARY CONFLICT – CONCEPTUAL DELIMITATIONS

In the first decades of the 21st century, some of the vulnerabilities, risks and threats to the security environment do not have a well-defined outline, as they are highly uncertain. In this complex, dynamic and conflicting world, the confrontation is actually between different values and principles, between totalitarianism and democracy, between divergent interests, between nationalism and globalisation, between the way different religions perceive the truth etc. Although global developments offer new opportunities, they also pose many challenges to national values and interests. The strategic objectives seem to be achieved using new methods – based on the specifics of the current century.

The consistency and physiognomy of conflicts have changed drastically: new political-economic and strategic situations of insecurity, new means to achieve and fulfil various objectives, new technological means and means of action and innovative (plasma weapon, unmanned aircraft or automatic, aerial micro-vehicles, robot ships, low energy laser weapons, isotropic radiation emitters, non-nuclear electromagnetic pulses, high power microwaves, infrasound, super-caustic substances, adhesion reduction technologies, polymeric agents, simulation and illusion visual technologies etc.), creative power manifestation concepts, a different attitude towards the opponent, the most diverse spaces for action, a very wide range of dominant types of action and increasingly sophisticated and unexpected ways of manifesting violence (Popa, 2004, p. 9). Starting with the example of annexation of Crimea by the Russian Federation and continuing with the tensions between Ukraine and the Russian Federation, US-China economic tensions in the case of Huawei, economic restrictions imposed on the Russian Federation by the United States, confirmed cyber-attacks in various European countries, trade conflicts and how the relevant actors in this field communicate, the case of poisoning of Sergei and Iulia Skripal, the case of Pizzagate (fake news), Cambridge Analytica, the potential involvement of the Russian Federation in the presidential elections in the United States, the reflexive control used by the Russian Federation with an impact on both the military and civilian life) etc. – all these are illustrations of the different forms of manifestation of the conflict specific to the current century.

Contemporary conflict uses as raw material vulnerabilities specific to those living in the 21st century: dependence on technology, exclusive information from the online environment, excessive use of social networks, the power of opinion formers, the uncontrolled speed of spreading the information distributed on digital platforms, with the ability to amplify and disseminate information instantly, without any editorial or human filter, the fake-news phenomenon etc. These vulnerabilities create serious security breaches that different actors use to achieve their goals: recruiting, forming opinions, influencing, misinforming, increasing or decreasing the confidence of the target audience using security breaches in different environments, creating seemingly non-existent problems between (two) other actors, creating mistrust in an existing partnership or one that is to be created, commercial purposes etc. In the current context, there are actors who face many economic and social problems, political difficulties, ethnic and religious rivalries, territorial disputes, problems accentuated by gaps specific to the 21st century.

There is a tendency to interconnect a multitude of dimensions, developing a concordance between the military dimension and the political-diplomatic, psychological, economic, informational approaches etc. of a respective state actor; the society in which we live will have as a confrontation area the virtual, cultural, motivational space. The dynamics of the struggle is based on the manipulation of information, mentalities, interests, expectations by influencing morale, mood. These will be used to create an increased degree of uncertainty to achieve the desired effect; both individual behaviour and especially collective behaviour are much easier to control with the means specific to the 21st century (Topor, 2018, pp. 11-19).

Another factor specific to current conflicts is the *growing importance of alliances*. Alliances have become a means of achieving interests, goals, reaching to some extent to influence the world order. Nation states remain a subject of international law, but they cannot achieve complex objectives or solve complicated problems alone and are therefore obliged to integrate into international security structures. Thus, the main reason why states are part of alliances is the desire to maintain their national security and integrity, as well as their sovereignty. As members of an alliance, apart from the obligations, actors have certain advantages and a power derived from group membership.

Contemporary conflict avoids forceful impact with the adversary, counteracts or compensates for his superiority and exploits weaknesses in security systems, deceives the adversary's vigilance, plays and undermines concrete actions, uses non-standard forms with a huge psychological impact on the ability to counteract. In this type of conflict, the focus is on creating a state of chaos; media, in all its forms (audio, television, internet, print media etc.), plays a key role in this (unfiltered news can form or distort the truth, which will become more and more subjective). Actors who have the technological and informational power and the ability to transmit information so that the target audience will act according to the wishes of the initiators (manipulating behaviours by using information) will take benefit from that.

Confrontations specific to the last century are no longer found in the current reality; more recently, there has been a shift towards confrontation between irregular forces, with guerrilla fighters, terrorists, ethnic and religious elements etc.

The old world order, based on bipolar logic (characteristic of rivalry and capacity for mutual annihilation of some states) no longer responds to current threats, therefore the efforts of the international community are focused on trying to find the right methods to counter new and compressed threats. We call it *contemporary conflict*.

Almost all local post-war conflicts have the characteristics of asymmetric conflicts, led by one of the two rival world superpowers: the United States of America and Russia. The evolution in different fields has brought new types of threats, specific to the 21st century; the threats of the current century have highlighted new vulnerabilities and risks globally. Given the specifics of the current century, current conflicts can fall into the following typology:

- military conflicts fuelled by religious differences;
- inter-ethnic military conflicts;
- military conflicts of economic causes (Buzea, 2015, p.71).

Saida Becar advances three forms in which military strategy can be identified (Saida, 2001, p. 31):

- symmetry, which involves the armed opposition of two approximately equal forces in terms of development, composition, equipment (war fought face to face in which surprise is achieved through the originality of operational strategies);
- dissymmetry, which implies quantitative and/or qualitative superiority of one of the parties;
- symmetry, which involves gaining an advantage by exploiting the weaknesses and vulnerabilities of the opponent (total discrepancy between the goals, objectives and means used, courses of action used by opponents).

Contemporary conflict has an asymmetrical characteristic; the asymmetry in the contemporary conflict is represented by flexibility, the key ingredient, the situational-adapted conception that maximises its own advantages and exploits the opponent's vulnerabilities; also, through asymmetry, a relevant increase in efficiency is obtained, the aim being to obtain maximum results with minimum human and material efforts and losses, but which implies a maximum effort of intelligence and creativity (Braun, 2004, p. 222).

The operational strategic objective is different for each type of conflict; while symmetrical conflicts seek to neutralise the opponent's forces, asymmetrical conflicts also seek to change the opponent's psychology in order to cause it to give up the fight in which it did not even sign up, so that it can later be willing to negotiate from a disadvantaged position.

Among the specific goals/objectives of asymmetric conflicts, we find (Buzea, 2015, p. 72):

- penetration of the centres of political and social power through mass-media;
- undermining, enslaving, destroying the economy of a target country;
- changing the system of principles, values (religious, traditional etc.);
- changing the national interests specific to a certain actor/state;
- obtaining economic advantages (areas rich in strategic resources are targeted);
- decreased confidence of the target population in the command centres;
- change of leadership (change of governments, political regime) in a certain state;
- division of states, formation of new states etc.

At the same time, we can observe that another characteristic of the contemporary conflict is the *specificity of the actors involved*: if, in the 20th century, state actors were those who fought for power, we are now witnessing a major change in international relations. In the 21st century, non-state actors are all those who do not represent a state, but who have the power to operate internationally and also have relevant potential of manifesting power at regional or global level. Anne Thompson-Feraru, in her paper entitled *Transnational Political Interests and the Global Environment*, grouped them into several categories:

- international governmental organisations (IGOs);
- international non-governmental organisations (INGOs);
- corporate interest groups (IGC) and transnational corporations (TNCs);
- epistemic communities (EC);
- a special category that includes terrorist groups, professional organisations, religious groups etc. (Thompson-Feraru, 1974, pp. 31-60).

Today, there are tens of thousands of transnational corporations operating around the world that, theoretically, do not officially participate in political decisions, but obviously act to impose their own interests. These non-state actors act discreetly and often form teams to have more power than a state actor can imagine.

Given the rapid evolution of technology, it is difficult to estimate trends when it comes to security threats, beyond a 10-year horizon. However, the relevant key words are: unconventional, asymmetric actions, fight against civilisations and transnational terrorism, technologies without human operators, media influence, recruitment in religious and ethnic groups (religious extremism), fear, horror, state of insecurity, generalised insecurity, unpredictability of actions etc.

The concept of power must also be adapted to the characteristics of the 21st century. At present, not only state actors can participate in relevant decisions; the peculiarities of the current century allow the participation of non-state agents; terrorist, multinational financial or transnational groups can have a major impact on the policies of a particular state. The contemporary conflict represents a sum of actions carried out in all the fields of activity.

Contemporary conflict involves actions in several of the military and non-military areas, an indefinite period of time and a not very clearly delimited space of development from a geographical point of view; in this context, the delimitation between war and peace is very difficult to make.

In this type of conflict, strategic communication is the centre of gravity, the core through which objectives in different areas are met (alongside with the military or economic instrument). Narrative strategies specifically designed to influence behaviours, change perceptions and attitudes are methods of shifting poles of power, polarising opinions, influencing the trust and support of targeted audience segments in certain authorities, or creating social imbalance which may subsequently facilitate the achievement of other objectives.

STRATEGIC COMMUNICATION IN CONTEMPORARY CONFLICT

In recent years, strategic communication has become a very popular topic in itself. However, the different use of the term strategic communication has led to a considerable level of confusion. There are currently many contradictions regarding the definition and role of strategic communication, both academically and militarily.

I will briefly refer to some approaches to strategic communication and later give examples that demonstrate the role of strategic communication in contemporary conflict. Through argumentation and logical-deductive reasoning the new perspectives of the conflict in the modern combat environment are approached and the presence, role and tools of strategic communication are highlighted, in the context of the new security threats and the impact the online environment has in contemporary conflict.

Strategic communication, conceptual delimitations, examples

The first relevant official document that mentions the role of *"strategic communication"* in promoting the values of a state in the world is the US National Strategy for Public Diplomacy and Strategic Communication, from 2007. This document mentions the US security objectives, according to the Security Strategy national law of the United States: promoting human dignity; strengthening alliances against terrorism; defusing regional conflicts; prevention of threats posed by weapons of mass destruction; encouraging the development of the global economy; expansion of developed areas; cooperation with other centres of global power and the transformation of US national security institutions to meet the challenges and opportunities of the 21st century (Deac, Buluc, 2019, pp. 40-41).

According to Professor Denis Murphy, a member of the United States Army War College, *"strategic communication is an emerging concept, defined in various ways, devoid of doctrinal basis, and with a lexicon that fails to provide a unitary understanding"* (Paul, 2011, p. 17).

The recent edition of NATO's Strategic Communication Policies considers that, in the context of the Alliance's military activities, strategic communication *"integrates communication capabilities and public intelligence personnel with other military activities to understand and shape the information environment, in support of NATO objectives and goals"*. (p. 4). According to the mentioned doctrine, the implementation of strategic communication requires a combined effort and is based on the following principles:

- activities based on NATO values;
- activity dictated by the objectives derived from the narrative strategies, doctrines and strategy initiated by the politico-military framework;
- credibility and trust are fundamental attributes and must be protected;
- words and actions must be in line;
- the information environment must be understood;
- communication is a collective and integrated effort;
- the emphasis is on achieving the desired effects and results;
- communication is allowed at all levels (Ibid.).

Christopher Paul defines, in his 2011 paper, strategic communication as: synchronizing words and deeds and how they will be perceived by selected audiences as well as programs and activities deliberately created to communicate and engage targeted audiences, including those implemented by Public Affairs, Public Diplomacy and Information Operations professionals (Paul, 2011).

In an official document from the United States Department of Defense, strategic communication is discussed as a process and not a set of discrete capabilities, organizations, or activities. Strategic communication is defined as the process of integrating the perception challenges of the targeted audience segments into a policy of creation, planning and action at each level (Department of Defense, 2009, p. 1).

In the US view, strategic communication is defined as: *"The United States Government's focused efforts to understand and engage key audiences to create, strengthen, or maintain conditions favorable to the promotion of the interests, policies and objectives of the United States Government through the coordinated use of programs, plans, themes, messages and products in sync with the actions of all instruments of national power"* (Department of Defense Dictionary of Military and Associated Terms, 2017, pp. 223 -224).

Examples that demonstrate the role of strategic communication in contemporary conflict

The communication process is a basic feature of almost all confrontations between global or regional actors. What differentiates the way it manifests itself, over time, are the methods and strategy adopted to achieve the proposed objectives. From war propaganda to disinformation campaigns encountered over time in confrontations in various areas of the operational environment of conflict manifestation, the role of communication in the manifestation of conflicts has changed.

In order to maintain its applicability and achieve the expected effect among the population, it is easy to see that war propaganda specific to the conflicts of the 20th century is found in a manner adapted to the context of contemporary conflicts. Both propaganda and disinformation need propagandists, re-transmitters; one of the basic missions of propaganda thus becoming to recruit, to gain new faithful and devoted supporters and people of action.

Time spent on social networks, communication and information exclusively online may be considered a vulnerability of those living in the 21st century, which different actors use to recruit, form opinions, influence, disinform and increase or decrease the confidence of the target audience using security breaches in different environments.

Strategic communication, no matter how it is found, aims at social influence. Narrative strategies, themes and lines of persuasion, the use of vulnerabilities of certain audience segments are just some of the stages that are part of the complex process of strategic communication.

In order to be able to influence perceptions, to be able to change attitudes and behaviours, an analysis of the target audience must be made in order to subsequently formulate appropriate messages to ensure that the desired effects are achieved. To this end, it is necessary to know in detail their vulnerabilities, preferences, desires, fears. The economic, religious, cultural, political, military etc. context must also be taken into account. Changing the perceptions, attitudes, behaviours of an audience can be a long process (Psychological Operations, 2018).

In the current context, strategic communication has become a necessity, given the exponential development of social media, the intensification of online disinformation campaigns, the diversification of the means, sources and targets of manipulative influence campaigns. For a state actor, strategic communication is also the process designed to counteract the destructive effects of misinformation and malicious information, targeting not only the external public, in order to promote national interests, but also the internal public, in order to increase its resilience to information attacks (Deac, Buluc, 2019, p. 46).

An efficient use of power is achieved by using strategic communication. For example, American cinema, which has remarkably and successfully promoted US values, has led to behaviours favourable to American interests not only in Europe, but also in the Far East. Strategic communication is a prerequisite for the success of the war on terror because it requires the voluntary cooperation of other people, institutions and nations (Eric X. Li, 2018).

Also, for a better understanding, a special importance must be given to the object on which strategic communication, with all its components, acts: people, constituted in groups, communities, masses, institutions and organisations. The masses or crowds are targeted by propaganda, based on favourable events or circumstances that facilitate the achievement of the goal precisely by presence.

As it has already been mentioned, strategic communication has the ability to change poles of power, to, over time, turn sympathy into adoration and antipathy into hatred, to change beliefs, perceptions, attitudes and behaviours. An example in this regard is the strategic communication policy of the Russian Federation.

At present, the Russian international media is not, in itself, one of the most successful disinformation instruments in European countries; it is often a niche product (not the case, for example, in Serbia, but it is true for Estonia) targeting private groups. Much more important is the reflection and increasing distribution of content produced and distributed through populist groups, parties and social movements in the target countries and also the instrumentalization of Russian-speaking minorities, as in the case of Estonia or Germany (Meister, 2018, pp.11-23). If they are not the direct target of the disinformation strategy, the content of Russian disinformation and propaganda is spreading through these increasingly successful groups and networks. At the same time, not only party members but also leaders from some European countries use arguments about Russian misinformation and propaganda, while former politicians, journalists or pro-Kremlin pseudo-experts bring them to the media through interviews (Suslov, 2017, pp. 60-71).

Most elements of the narrative strategies promoted by the Russian Federation already exist in parts of European societies, which criticise the inability of governing elites to solve the problems of their countries in an increasingly complex world. This self-doubt is supported by the Russian international media, whose main goal is to *"build a counter-public and demonstrate the manipulation of the media"*. Through this policy, the Russian Federation instigates instability and polarisation of societies in order to claim power in the name of restoring stability.

Also, the close relations that the Russian Federation creates or maintains with certain NATO member states aim at dividing NATO by creating and highlighting misunderstandings between allies (Flanagan, Chindea, 2019, pp. 3-4). To meet these objectives, the Kremlin uses specific *soft power and* even *smart power* influencers, methods that include propaganda and influencing the information environment. Russia adapts both its narrative strategy and the methods of disseminating information to each state (Flanagan, Chindea, 2019, pp. 9-10).

The annexation of Crimea by the Russian Federation (2014) is a concrete example of the manifestation of contemporary conflict (hybrid warfare) and the importance of using strategic communication.

One of the ways chosen by the Russian Federation to threaten and discourage any possible intervention from the international community was by broadcasting a documentary entitled *Crimea, The Road Home* (Burke, 2017, pp. 31-32). On 15 March 2015, the Russian public television channel Rossiya 1 presented this film in which it is stated that Russia is ready to use nuclear weapons if the United States or its allies choose to intervene militarily in favour of Ukraine. To give strength and legitimacy to the Russian Federation's intervention in Ukraine, President Vladimir Putin said that in Crimea, Russia has already placed batteries of coastal missiles, systems installed in such a way that they can be seen from the sea and satellites, to discourage any attempt to attack the Peninsula. Following this political and military process, the Crimean Peninsula, then part of Ukraine, came under Russian control and was integrated as two federal subjects: the Republic of Crimea and the federal city of Sevastopol.

Although international organisations (European Union, United Nations etc.) almost unanimously opposed this action by Russia, the measures were limited to economic sanctions and political, diplomatic, non-military action.

In this very brief analysis, we saw the importance of strategic communication in a contemporary conflict. Although threat and deterrence are specific elements of strategic culture, this conflict, a conflict with resonance specific to the 21st century, intertwined these two techniques with political movement, mass influence, strong diplomatic discourses, cultural similarities through the large Russian population residing in Crimea.

CONCLUSIONS

From the aspects presented above, we consider the following basic characteristics to describe the contemporary conflict:

- strong uncertainty;
- unpredictability;
- chaotic character;
- the tendency to demilitarise;
- asymmetric character.

Using these characteristics as a starting point, the contemporary conflict develops in the current context of the specificities and/or vulnerabilities of the

21st century:

- the dominant role of the media;
- the defining role of the political factor;
- progress in the technological sphere – massive integration of technologies;
- the growing importance of alliances, the development of alliance and coalition strategies;
- the importance and growing power of non-state actors;
- the importance of the opponent's psychology and how this aspect can be used to fulfil certain objectives (division and demoralisation of the opposing population through disinformation campaigns).

Strategic communication is an essential element in contemporary conflict through its ability to change poles of power, perceptions, attitudes and behaviours. The examples given in the previous chapter provide a basic understanding of how strategic communication can meet certain international goals of state actors at national or international level. We live in a complex world, where the form of conflict is no longer the conventional one. In this type of conflict, strategic communication is the centre of gravity. Power manifests itself and takes various forms, with courageous goals and not at all easy to notice. In this context, I consider it very important to pay more attention to the way in which the narrative strategies are presented, national objectives are promoted and to the way in which values of different global or regional actors are consolidated.

BIBLIOGRAPHY:

1. Albert, M. (1994). *Capitalism contra capitalism*. București: Humanitas.
2. Atanasiu, D. (1997). *Momente ale artei militare contemporane*. București: Editura Militară.
3. Attali, J. (2007). *Scurtă istorie a viitorului*. București: Poliro.
4. Bârgăoanu, A. (2018). *#Fake news, Noua cursă a înarmării*. București: Evrika.
5. Bedar, S. (May, 2001). *L'asimetrie comme paradigme central de la Strategie americane*, în *Le Debat Strategique*, no. 56.
6. Buzan, B. (1991). *Popoarele, statele și teama*. Chișinău: Cartier.
7. Buzea, C. (2015). Sesiunea de comunicări științifice, Securitatea națională, europeană și euroatlantică, vol. II, București: Universitatea Națională de Apărare , *"Carol I"*.
8. Burke, J., Panina-Burke, A. (2017). *The reunification of Crimea and the city of Sevastopol with the Russian Federation*. Moscow: Russian Law Journal, Vol. 5.
9. Braun, N., Măciucă, M., Toma, G. (2004). *Managementul insecurității la început de secol informațional, provocator, nesigur*. București: Scaiul.
10. Chiriac, D., Manta, D., Emil, I. (2007). *Conflictul militar în epoca contemporană*. București: Universitatea Națională de Apărare *"Carol I"*.
11. Deac, I., Buluc, R. (2019). *Dezvoltare conceptuală a comunicării strategice în domeniul securității*, Impact Strategic, no. 1-2(70-71)/2019, București: Universitatea Națională de Apărare *"Carol I"*, Centrul de studii strategice și securitate.

12. Flanagan, S., Chindea, I. (2019) *Russia, NATO, and Black Sea Security Strategy-Regional Perspectives from a 2019 Workshop*, prepared for the U.S. European Command, Santa Monica: RAND Corporation.
13. Gray, S., C. (1999). *Modern Strategy*, New York: Oxford University Press;
14. Gray, S., C. (2000). *Războiul, pacea și relațiile internaționale*, Iași: Polirom.
15. Hoffman, D., E. (2010). *The Dead Hand: The Untold Story of the Cold War Arms Race and Its Dangerous Legacy*. Washington: Doubleday.
16. Hofstede, G., Hofstede, J., G., Minkov, M. (2012). *Culturi și organizații. Softul mintal*, translated by Mihaela Zografi, București: Humanitas.
17. Mureșan, M., Văduva, G. (2004). *Războiul viitorului, viitorul războiului*. București: Universitatea Națională de Apărare *"Carol I"*.
18. Panait, I. (2013). *Transformarea conflictelor și evoluția luptei armate după Războiul Rece*. București: Universitatea Națională de Apărare *"Carol I"*.
19. Paul, C. (2011). *Strategic communication. Origins, concepts, and current debates*. California: Praeger.
20. Popa, V. (2004). *Tehnologie și inteligență în conflictele militare*. București: Universitatea Națională de Apărare *"Carol I"*.
21. Suslov, M. (2017). *Framing and foreign policy: Russian media control and human rights*, in Shifting Power and Human Rights Diplomacy- Russia, Edited by Doutje Lettinga & Lars van Troost. Netherlands: Amnesty International.
22. Suvorov, V. (2010). *Spărgătorul de gheață*, Iași: Polirom.
23. Thompson-Feraru, A. (1974). *Transnational Political Interests and the Global Environment*. International Organization, Vol. 28, No. 1.
24. Topor, S. (3/2019). *Forme de manifestare a terorismului cibernetic*. București: Buletinul Universităţii Naţionale de Apărare *"Carol I"*.
25. Topor, S. (3/2018). *Informaţii despre ameninţări şi menţinerea controlului într-un mediu conflictual modern*. București: Buletinul Universităţii Naţionale de Apărare *"Carol I"*.
26. Tzi, S. (1976). *Arta războiului*. București: Editura Militară.
27. Voicu, M. (2018). *Matrioșka mincinoșilor. Fake news, manipulare, populism*. București: Humanitas.
28. Volkoff, V. (2017). *Tratat de dezinformare*. București: Antet.
29. *Department of Defense, Report on Strategic Communication*, Washington, DC, (March 2010).
30. *Department of Defense Dictionary of Military and Associated Terms* (2017).
31. *MC 0422/6- NATO Military Policy on Strategic Communications*, North-Atlantic Council.
32. NATO Military Policy on Strategic Communications.

WEB SOURCES:

1. https://www.ssoar.info/, retrieved on 12 August 2020.
2. https://foreignpolicy.com/, retrieved on 23 September 2020.
3. http://stratcom.nuou.org.ua/, retrieved on 23 September 2020.
4. https://shape.nato.int/, retrieved on 29 September 2020.

SOCIAL MEDIA AND THE THREATS AGAINST HUMAN SECURITY DEEPFAKE AND FAKE NEWS

Colonel Prof. Filofteia REPEZ, PhD

Assoc. Prof. Maria-Magdalena POPESCU, PhD

Faculty of Security and Defence, “Carol I” National Defence University, Bucharest

The proliferation of unconventional weapons triggered by technological progress have raised the threat level for individual and society through the uncertainty generated by managing words and images, through AI algorithms and through social engineering techniques. The rapid growth of social media has allowed for the information to be disseminated and identified in a reckless manner. Deepfake, centred on economic or political attacks, and fake news, acting on democracy and social systems, are the products that state and non-state actors use, which are aimed at weakening security in general and human security in particular. Deepfake and fake news as main instruments for hybrid warfare have become important topics for security culture. In terms of human security, social media generates series of advantages, however, whatever is developed through the hostile use of these networks generated series of threats for societies. Starting from these aspects, the present paper provides, along with conceptual definitions, a general understanding on the implications that social media challenges have on human security.

Keywords: social networks; deepfake; fake news; security culture; human security;

INTRODUCTION

Skyrocketing proliferation of apps that encourage communication and syndicalization generate, alternatively and simultaneously but detrimentally, common spaces where performing activities as those mentioned above, based on certain skills, turn them into vulnerabilities. Facebook, Twitter, LinkedIn can often represent security risks and threats. A study in 2011 (Ponemon) related to the security problems that social media can generate, performed in twelve countries, indicate the fact that more than 50% of the respondents reported frequent cyber-attacks especially in the apps used for communication of both state and non-state actors, while studies performed by Kaspersky Labs (2009) show that social networks are ten times more efficient in distributing malware and other types of threats (Ibid.), supporting the ideas with about 45.000 hostile folders identified as shared in social media.

The diversity of threats is on the rise, keeping up with the technological progress which is cheaper and cheaper due to Artificial Intelligence support. Among inordinate types of threats one can count a low level in authentication measures, information leak, social engineering attacks like *phishing* (fraudulent data theft) *spear phishing* (targeted attacks to destroy a system or data mining), *baiting* (personal data extraction under the false bounty promises), *scareware* (posts or messages that bombard victims with false alarms and fictive threats, deception) and web app attacks (Jakobsson &Myers, 2006).

Social engineering attacks whose life cycle is presented in *figure no. 1* (based on *Impreva*) exploits people’s trust in their peers (Granger, 2002), which facilitates the message proliferation speed as well as the dimension of the impact on human security.

All these methods, together with many others, act based on a very well determined plan, identifying victims, gathering intelligence about them so that they can, afterwards, send customised attacks through engagement or through generating a narrative that can attract the target whose personal security, economic, political and social coordinates can then be destabilised. Using these narratives with aids from machine learning to generate propagandistic campaigns are extremely frequent in virtual space nowadays.

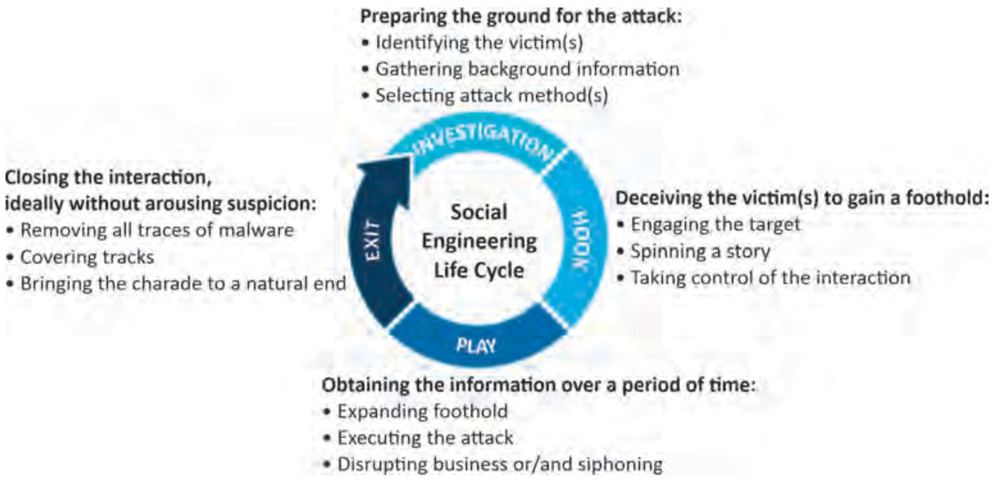

Preparing the ground for the attack:
• Identifying the victim(s)
• Gathering background information
• Selecting attack method(s)
INVESTIGATION
Closing the interaction,
ideally without arousing suspicion:
• Removing all traces of malware
• Covering tracks
• Bringing the charade to a natural end
EXIT
Social
Engineering
Life Cycle
HOOK
Deceiving the victim(s) to gain a foothold:
• Engaging the target
• Spinning a story
• Taking control of the interaction
PLAY
Obtaining the information over a period of time:
• Expanding foothold
• Executing the attack
• Disrupting business or/and siphoning

Figure no. 1: Lifecycle of a social engineering attack

Concepts like *deepfake* (concept that relates to any fake, audio or video, created through the use of neural network techniques inside machine learning as well as through generative adversarial networks – GAN responsible with ensuring that the deepfake is impossible to be identified) or *fake news/disinformation* (targeted disinformation campaigns meant to bewilder society in favour of political gains, manifested through intentionally flawed disseminated as valid information, especially since it has been proved that bots – software app that operates repetitive tasks like automatically generated messages, promoted ideas, user following techniques or fake accounts that lure virtual identities of the current accounts – disseminate fake and real articles at similar speed, fake ones spreading six times faster than the true ones (Fillion, 2018), to produce human security attacks from a variety of angles – economic, social, political, individual.

HUMAN SECURITY – A BENCHMARK ON SECURITY AGENDA

The new approach over security according to the UN Programme for Development (UNPD) was included in the human security concept detailed in the 1994 Human Development Programme, stating that *"human security is relevant for people everywhere, both in rich and poor countries"* (Kaul et al., 1994).

This report highlights the seven components of human security: *economic security* (ensuring a minimum wage for every human being); *food security* (physical and economic access to basic foods, anytime); *health security* (ensuring a minimal medical protection); *environment security* (protection from natural disasters or environmental damage implications); *personal security* (protecting individuals from violence, especially from physical violence); *community security* (protecting communities and their members to maintain and replicate their traditional values and relationships); *political security* (ensuring a life standard in agreement with fundamental human rights, as well as ensuring individual and group freedom in front of any governmental essays to control them). This document regulates human security as a benchmark for a new security agenda and it has gradually become a key concept in international security agenda (Edstrom, 2011). Human security thus highlights the trifold relationship (*figure no. 2*) between security, development and human rights and considers that these are the basic elements for human security and national security.

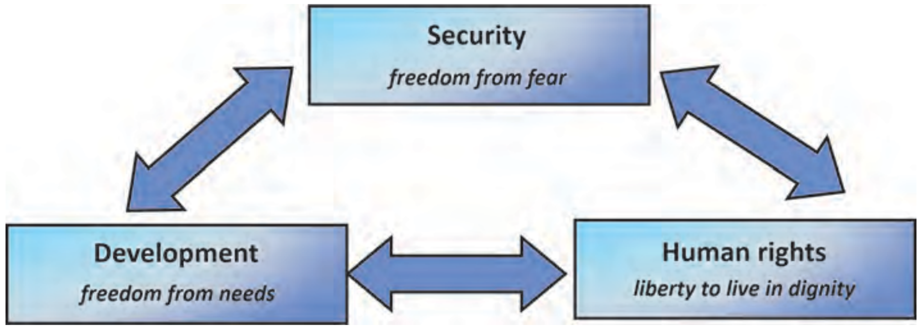


Figure no. 2: The human security trifold relationship (Edstrom, 2011)

Human security complements national security, improves human rights and consolidates human development; human security means protection of the fundamental rights and freedoms that are essential to life.

In this context, human security has become a new field of study, a sub-chapter of security studies and gradually this field has proven itself to be a complex one, especially in pragmatics and dynamics, as well as one under constant development. The irrefutable technological progress has major impact on all walks of life and on national and international security, for society and individuals. Hostile, malign, foreign and domestic actors manipulate truth by distorting information, avoiding topic, by facts and opinion gaming as well as by appealing to artificial intelligence products, all to undermine social resilience. An extremely prolific environment for all those mentioned as skyrocketing opportunities to replicate and disseminate but also to believe and validate, aided by knowledge groups, is the social network.

FROM SOCIAL NETWORKS' POSITIVE EFFECTS TO DEEPFAKE, FAKE NEWS AND THEIR IMPACT ON HUMAN SECURITY

Internet access has become a defining and reforming phenomenon of the present times and it thus involves communication instruments, common interactive spaces, a research environment and infinite possibilities for reality replication, with an effect on human security seen in its complexity. According to statistics, approximatively 4.57 billion people (*figure no. 3*) i.e. 59% of the world population were using the internet in July 2020, while the figures are continuously going up.

Emergent technologies, open sources and the ubiquity of access allow dissemination and multiplication, co-creation and co-participation, which, aided by artificial intelligence, by software agents that learn users' activities and users' physiognomy, their reaction as well as their online behaviour in order to replicate them, have turned social media in an unprecedented phenomenon and have revealed opportunities, risks and challenges for millions of people worldwide, not only through connectivity and closure among users but also through enhanced targeted attacks due to sensitive information availability and large users' database. In this respect, estimates show that the number of social media users reached 3.5 billion in April 2019 (Clement, 2020).

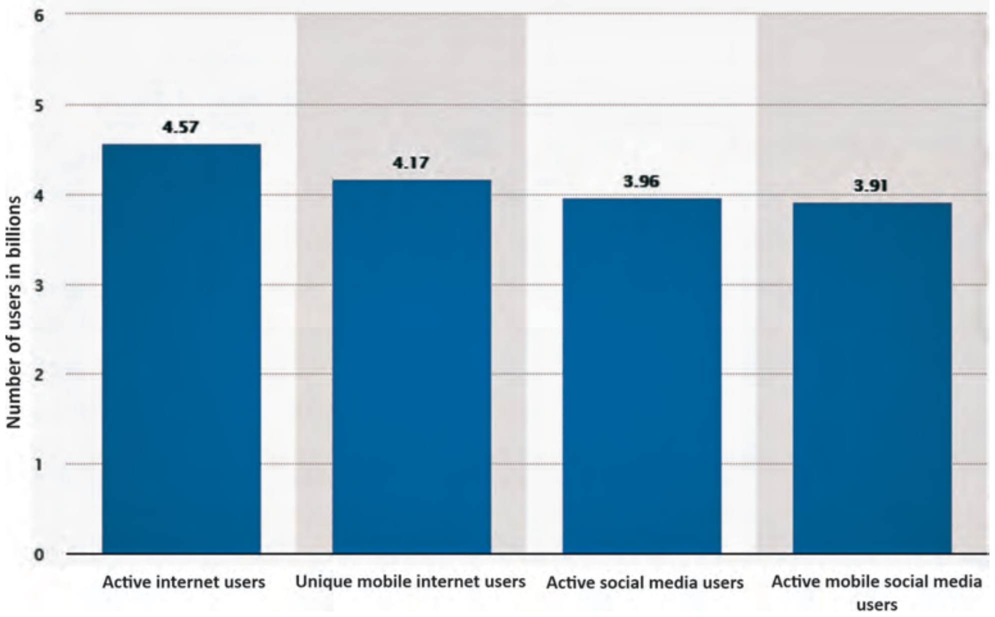


Figure no. 3: Digital population worldwide – July 2020 statistics (Clement, 2020)

Starting with a positive influence on human security especially over personal and health security components, social media proves its impact especially over people in their 40s to 70s, based on statistics (Fineberg, 2018). For example, 64% of the US citizens aged 50 and over, and 37% of the US citizens aged over 65 use social media regularly (Sauer, 2020).

Focusing on spatial proximity, in Romania, a valid example is the blog *"The fourth age"*, belonging to Pompiliu Sterian (Vlad, 2018), resident of Moses Rosen Home. His involvement in the project and the use of blogging bring inordinate benefits: a change in perception over the old age concept by encouraging a positive approach over time stages, group creativity stimulus, an archive of personal and collective life stories.

On the other hand, an excessive use of social media impacts personal health security: we mention here passive users, easy and safe targets for attacks that are aimed at trust fading, anxiety generated by poor sleep quality, weak self-confidence along with shallow attention, poor observation and hyperactivity – all these are factors that facilitate extremist group head hunting. One can mention here an impact on academic performance as well through the effect on users' health – a mental torment called Pathological Internet Use (PIU), complemented by the consideration that Facebook has become a power instrument par excellence which indirectly manipulates through virtual community and develops dependence, while social media lays marks over human security component (health security and personal security) a vision endorsed by Virgiliu Gheorghe, MD, biophysicist and doctor of bioethics (Andreiana, 2018).

Beyond the benign implications which excessive use of the Internet has over human behaviour and over users as social beings, over personal and health security, the daily appearance and the social media-defined modus vivendi expose users to other types of dangers, generated by those behind the barricade, the actors that generate hostile, malign content. The deepfake and fake news are the most frequently disputed and the most complex danger in terms of collateral effects.

Deepfakes or fake videos are created using an automated learning process (machine learning) called generative adversarial network (GAN), more exactly an algorithm which generates new types of data from the already existing ones. The video with Barack Obama or the one with Donald Trump who informally states that he withdraws the US from the environment agreement with France are among the most widely commented (von der Burchard, 2018). Moreover, a new technique that produces deep video portrait manifests itself as a facial ventriloquism which helps a person, a user to control the mimicry of another person, thus being able to say or do something at the initiator's command. Deepfake affects the democratic process with political and social ramifications and generates a reality apathy through which constant contact with disinformation determines users to lose confidence in what they see or hear, leading to a phenomenon in which individuals will consider all that surrounds them as being fake information. Predictions state that 2020 is a year when deepfake as a process and product is very often employed, especially since biometric data are more and more frequently approached as authentication instruments (*The Medium*, October 2019). Moreover, cybercrime experts improve deepfake characteristics to imitate individuals for financial frauds (Poremba, 2020). Thus, the problems with deepfake will be even bigger and more numerous since facial recognition such fake video rely upon is more and more used to unlock phones or to identify individuals at immigration points in airports, all these triggering numerous fraud opportunities.

In relation to these, the *McAfee* experts consider that the technological progress sustains both the positive and the negative agents' impact and this means solutions will be found by those who generate deepfake to avoid facial recognition agents (Povolny, 2019). This technology that impacts human security will bring difficulties in law enforcement as well. Consequently, public video comments can be used as a source for automated learning which can thus develop a deepfake video representing a person uttering the words that have previously been spoken by someone else. This way, individual's security, words and personal identity attribution are under larger and larger threats.

On the other hand, using fake news and disinformation in social media on an extremely often base represents threats to social stability, to economic development and democracy. Fake news as a term can hardly be defined due to its complexity (Wardle, 2017, Zuckerman, 2017, Danah Boyd, 2017, Jack, 2017), since it simultaneously triggers disinformation, misinformation and mal-information, with differences in the way the message meant to deceive is built. Disinformation is deliberately meant to produce cognitive imbalances while the one who sends the message is aware of the disfavour he produces; misinformation sends an information that is false by omission, ignorance or any other factor that comes in between delivering the message, in a truncated manner, while the one who disseminates it is convinced that he sends the truth, even though the message is false; mal-information, on the other hand, covers real assertions but which will impact people and situations negatively, in a hard way, once made public.

A 2018 UNESCO vision, *figure no. 4* presents the relationship between types of content in fake news, as they are defined above, and their modus operandi, together with the common elements they share. Among the reasons why disinformation is produced one can count financial causes, power lust in politics, nationally or internationally or social conflicts. Mis-information is based on socio-psychological reasons – the desire for social or political connection, for common beliefs or shared values (vaccine, religion, climate change); conversely, mal-information is based on information twist, on re-contextualisation. Together, all these impact fundamental rights, freedom of expression and democracy.

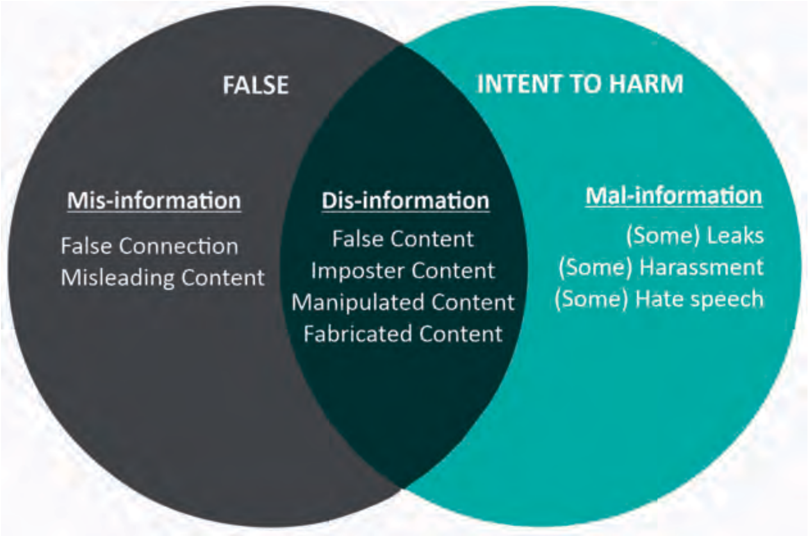


Figure no. 4: Fake news manifestations and their effects

To counteract them, inordinate detection softs and procedures that are intensely disseminated to identify and isolate disinformation have brought to life a new area of research called *Cognition Security – CogSec*, which studies the impact of all that falls under the general umbrella of fake news, with impact on human cognition (one can mention here misperception, uncertain acquisition of cognitive elements, adapted and directed formation or change of opinion with the intention to change behaviour, to develop a biased attitude in the decision-making process, to establish measures that fight back). Moreover, studies over cognition and memory try to explain how this type of information acts upon individuals and what it is that makes them be so easily trapped into believing the content.

The fact that individuals nowadays rely heavily on social information and on a set of anxieties that contextualise the errors, manipulation and influential waves, the information storm (Chatfield, 2019) as an alternative to irrational narratives applied in the fake news context and online division explains the inclination individuals have to fall pray for fake news phenomena more and more. Fake news as a phenomenon is based on individuals' incapacity to process the huge information wave which they have to manage daily. This incapacity generates the tendency to let ourselves driven on co-participants' decoding of data flow, at least for those sequences which we do not have to check and for whose explanation we lack the critical thinking skills to validate (when we possess insufficient knowledge to question ourselves). The agents that generate fake news have, among the political, social, economic and demographic interests, financial ones that turn billions of data into profit. The traffic of posts, rating, appreciation or sentiment analysis monetise reputation. The carelessness that characterises the way information is processed or selected from the abundance of news in social networks, slow thinking or simply an alignment to opinion and values that are shared within a group are just a few of the reasons added to the list of decoding and confirmation biases, along with the crowd illusion, post-factual analysis or retrospective bias, along with the decision-making fatigue (Baumeister, 2003) or cognitive load (Sweller, 2010), all these being facilitative elements for fake news victims.

Defined as the word of the year 2017 (*Collins Dictionary*, 2017), fake news pose health security problems (vaccines), environment security (climate change), political security (elections) and economic security (a stability in prices and shares). Among the examples for disinformation or propaganda with fake news that impact national and international security one thinks of the capital controls implemented by the Turkish government, with effects on national currency flow, which dropped by 20% compared to the US dollar, generating important economic consequences. A similar case was the one connected to Greek and North Macedonian border, when the information released had a strong consequence on the social security of directly involved refugees and immigrants. To all these, one might add the terrorist attack in Manchester, in 2017, when series of disinformation messages were spread about missing children and attackers roaming freely everywhere. In the context of disinformation Russia is a common denominator for most of the analyses, with frequent hints at trolls factories, while names like Sputnik and Russia Today are known as indicators that influence international public opinion (see the messages against Hillary Clinton etc.) (Vasu et al., 2018), thus touching upon democracy and individuals' collective decision rights.

CONCLUSIONS

The advancement in technology compared to human capacity to keep up with all the hidden facets artificial intelligence has, based on neural activity which exploits natural language processing within machine learning, makes for the few but complex products society faces today to have become irrefutable dangers for many of human security aspects. Volatility and versatility of the apps that generate malign communication products that accompany messages in daily mediated, mass social media – enhanced communication make deepfake and fake news to be the most frequent non-kinetic weapons in the information warfare, with an impact on human security. Fighting these should be through media literacy, through critical thinking and through gaining depth in a counter-clock race where human neural networks should at least keep up if they cannot do more, in surpassing machine learning natural language processing.

BIBLIOGRAPHY:

1. Andreiana, S. (2018). *Reţelele de socializare online şi influenţa lor asupra societăţii*. Virgiliu Gheorghe, MD: *"What we live today is another type of communism"*, https://evz.ro/retelele-socializare-online.html, retrieved on 3 August 2020.
2. Boyd, D. (2017). *Google and Facebook Can't Just Make Fake News Disappear*, Wired, https://www.wired.com/2017/03/google-and-facebook-cant-just-make-fake-news-disappear, retrieved on 23 September 2020.
3. Von der Burchard, *H. Belgian socialist party circulates 'deepfake' Donald Trump video*, https://www.politico.eu/article/spa-donald-trump-belgium-paris-climate-agreement-belgian-socialist-party-circulates-deep-fake-trump-video/), retrieved on 23 July 2020.
4. Edström, B. (2011). *Japan and the Challenge of Human Security. The Founding of a New Policy 1995-2003*. Institute for Security and Development Policy.
5. Fillion, R.M. (2018). *Fighting the Reality of Deepfakes*. Nieman Lab, https://www.niemanlab.org/2018/12/fighting-the-reality-of-deepfakes/, retrieved on 11 September 2020.
6. Fineberg, N.A., Demetrovics Z., Stein, D.J., Ioannidis, K., Potenza, M.N., Grünblatt, E., Brand, M., Billieux J., Carmi, L., King, D.L., Grant, J.E., Yücel, M., Dell'Osso, B., Rumpf, H.J., Hall, N., Hollander, E., Goudriaan, A., Menchon, J., Zohar, J., Burkauskas, J., Martinotti, G., Van Ameringen, M., Corazza, O., Pallanti, S., Chamberlain, S.R. (2018). *Manifesto for a European Research Network into Problematic Usage of the Internet*. European Neuropsychopharmacology, Volume 28, Issue 11, 2018.
7. Granger, S. (2002). Social Engineering Fundamentals, Part II: Combat Strategies, www.securityfocus.com/infocus/1533, retrieved on 14 September 2020.

8. Jack, C. (2017). *Lexicon of Lies, Data & Society*, https://datasociety.net/pubs/oh/DataAndSociety_LexiconofLies.pdf, retrieved on 18 August 2020.
9. Kaldor, M. (2010). *Securitatea umană*. Cluj-Napoca: Editura CA Publishing.
10. Kaspersky Labs (2009). Kaspersky Security Bulletin: Malware Evolution 2008, www.securelist.com/en/analysis?pubid¼204792051, retrieved on 16 September 2020.
11. Kaul, I. et al. (1994). Human Development Report. New York: Oxford University Press,http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf, retrieved on 16 July 2020.
12. Ponemon (2011). Ponemon Institute Research Report: Global Survey on Social Media Risks Survey of IT & IT Security Practitioners, www.websense.com/content/ponemoninstitute-research-report-2011.aspx, retrieved on 13 September 2020.
13. Povolny S., (2019). Threat Predictions Report, https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-labs-2020-threats-predictions-report/, retrieved on 24 September 2020.
14. Roceanu, I., Dragomir, A.M. (2019) *Rețelele sociale și provocări la adresa securității naționale*. Sibiu: Editura Academiei Forțelor Terestre *"Nicolae Bălcescu"*.
15. Sauer, A. (2020). 6 Must Follow Blogs for Seniors, https://www.leisurecare.com/resources/blogs-for-seniors/, retrieved on 05 August 2020.
16. Vasu, N., Ang, B., Terri, A.-T., Shashi. J., Muhammad, F., Juhi,A.(2018). *Fake news: National security in the post-truth era*. Policy Report January 2018, RSIS.
17. Vlad, R. (2018). *Bătrânul jurnalist de 99 de ani care a devenit blogger*, 10 April 2018, https://www.libertatea.ro/stiri/pompiliu-sterian-batranul-jurnalist-de-99-de-ani-care-devenit-blogger-2206322, retrieved on 5 August 2020.
18. Wardle, C. (2017). *Fake News. It's Complicated*, First Draft, https://firstdraftnews.com/fake-newscomplicated/, retrieved on 12 August 2020.
19. Zuckerman, E. (2017). *Stop Saying Fake News, It's Not Helping*. My Heart Is in Accra, http://www.ethanzuckerman.com/blog/2017/01/30/stop-saying-fake-news-its-not-helping, retrieved on 12 August 2020.

WEB SOURCES:

1. Global digital population as of July 2020 (in billions), https://www.statista.com/statistics/617136/digital-population-worldwide/, retrieved on 3 August 2020.
2. Social Engineering, https://www.imperva.com/learn/application-security/social-engineering-attack/, retrieved on 14 September 2020.
3. www. securelist.com/en/analysis?pubid¼204792051, retrieved on 14 September 2020.
4. www.websense.com/content/ponemoninstitute-research-report-2011.aspx, retrieved on 14 September 2020.
5. https://www.niemanlab.org/2018/12/fighting-the-reality-of-deepfakes/, retrieved on 14 September 2020.

6. http://www.operationspaix.net/DATA/DOCUMENT/4150~v~Japan_and_the_Challenge_of_Human_Security__The_Founding_of_a_New_Policy_1995-2003.pdf, retrieved on 14 September 2020.
7. https://reliefweb.int/sites/reliefweb.int/files/resources/91BAEEDBA50C6907C1256D19006A9353-chs-security-may03.pdf, retrieved on 14 September 2020.
8. https://www.leisurecare.com/resources/blogs-for-seniors/, retrieved on 14 September 2020.
9. https://www.rsis.edu.sg/wp-content/uploads/2018/01/PR180313_Fake-News_WEB.pdf, retrieved on 14 September 2020.

THE CONSTITUTIVE ELEMENTS OF THE CRIMINAL OFFENCE REPRESENTED BY COMMUNICATION OF FALSE INFORMATION. CASE STUDY: FAKE NEWS IN SOCIAL MEDIA

Gabriel-Bogdan CHIHAI, PhD Student
"Titu Maiorescu" University, Bucharest

In the present societal context, considering the tensions created among the population by the measures adopted by the Romanian Government in order to prevent the spread of the SARS-COV-2 virus, the correct and truthful information represents a primordial need for the people, who can be susceptible to the influences caused by any information, provided by any source. Without discussing about the psychological factors that determine people to give up to the filters through which they analyse information received in extraordinary situations, and taking into consideration the fact that the speed at which information is spread and consumed in the online medium, especially in social media, surpasses the speed at which information from official sources, which must be subjected to processes of approval, certification and signature, is spread, this research aims to create an incursion in the constitutive elements of the criminal offence represented by the communication of false information, in regard to the specific case of the spread of fake news in social media, with a potential effect on the national security.

Keywords: criminal offence; spread; fake news; social media; national security;

INTRODUCTION

In the year 2020, the whole world, including Romania, was subjected to great challenges in all fields of activity, from the SARS-COV-2 virus point of view. At national level, in order to exist the possibility to create the legal framework necessary for the prevention of the spread of this virus, the state of emergency was declared for a 30-day period (Decree no. 195/2020), that was later extended with another 30 days (Decree no. 240/2020). Because of the effects of the legislative instruments that were used in the time of the state of emergency for the restriction of citizen rights in order to prevent the spread of the virus, a prolific environment was created for the propagation of false news, also known under the name of *"fake news"*, phenomenon that can have negative effects against the national security. The lack of predictability of the measures and restrictions that were about to be adopted and made public, the necessity for adapting them on a daily basis depending on how the pandemic evolved, and the complicated process of signing, approval and publication of official documents, led to the situation in which the citizens were informing themselves from drafted normative acts, that were spread through social media (Facebook, WhatsApp etc.). The high level of trust that the people had in their colleagues or friends from their social media groups led to the fact that drafts of Government decisions, or those of the National Committee for Special Emergency Situations, spread in these groups, were considered as being authentic, especially that, most of the times, they were the normative acts that were adopted with little to no modification from the shared drafts.

One such case that provoked an immediate reaction from the population was that of *"Decision no.14 on 20.03.2020 of the Technical-Scientific support group for management of highly contagious diseases on the territory of Romania"*. This document, which contained drastic restrictions for citizens, was spread using the WhatsApp platform, in the morning of 20 March 2020. The document had a similar form to the decisions already adopted by the institution, even though it lacked the stamps and signatures that are specific to an approved document. Nevertheless, the document spread very fast, and a lot of the recipients considered that the document was authentic, thus creating a state of unrest among the population. Consequently, an intervention from the representatives of the issuing institution was mandatory, in order to explain that the document was just a draft for internal use only, that was subjected to study, and it produced no effects, because it was not approved at the time. Also, the decision to inform the criminal prosecution bodies, regarding the fact that a criminal offence was committed, namely the one stated by article 304 from the Penal Code (Law 286/2009) of distributing information that was not destined for the general public. Questionable is that the measures taken by the authorities, informing the criminal prosecution bodies about the offence previously mentioned, is enough in such cases, especially because the communication and spread of false news is covered by article 404 from the Penal Code (Law 286/2009). Thus, a more detailed analysis of the criminal offence previously mentioned is necessary, and the way in which *"fake-news"* from social networks, and their spread, grasp the limits of this criminal offence, and for the direct applicability of the analysed law principles, the case previously mentioned regarding *"Decision no.14 on 20.03.2020 of the Technical-Scientific support group for management of highly contagious diseases on the territory of Romania"*, will be of reference.

THE CRIMINAL OFFENCE OF COMMUNICATION OF FALSE INFORMATION/"FAKE-NEWS" JURIDICAL CONSIDERATIONS

Article 404 from the Penal Code regarding the criminal offence of communication of false information stipulates that: *"Communication or spread, through any means, of news, data or false information, or forged documents, knowing the fact that they are forgeries, and through which the national security is endangered, can be sanctioned with a sentence with one to 5 years of prison"*. (Law 286/2020). Right from the text provided for the article, it can be observed that the incrimination of acts that involve the communication of spread of fake news of information, with the condition that these endanger the national security. Verifying the prerequisites for incrimination can be made if the other constitutive elements of the criminal offence are met.

The object of the offence

The *legal object* is represented by the close connection between the right and the obligation of the Romanian state to have its information, data and documents protected, regarding their truthfulness and authenticity in the moments of disclosure. What should also be noted is the fact that in the majoritarian doctrine these data, documents and information are used not only with international organisations but also in the relationship of the state with its citizens, *"the creation of a frame of complete national security*" (Dobrinoiu et al., 2014) being an essential prerequisite.

In the analysed case, it is imperative o remark the fact that the data that is disclosed to the public and spread through social platforms and news oriented

web-sites, especially emphasises the relation of the state with its citizens, taking into consideration that at the moment of disclosure and spread to the public, on the Romanian territory it was established the state of emergency, and the restriction of citizens' rights was directly targeted by the document in discussion. Moreover, because in the clarifications from the Strategic Communication Group, it was mentioned that was just a draft (Strategic Communication Group, 2020), it cannot be denied that the state's right to have its documents protected was violated.

Material object

The material object of the criminal offence analysed through this research is, according to the doctrinal opinion (Dobrinoiu et al.), the medium through which the information, news or data are transmitted. To be remarked is the fact that in the case in which they are transmitted through spoken words, directly or through audio-video means, the criminal offence has no material object. The information, data and documents cannot be analysed distinctly from the medium on which they are found. The material object is therefore considered as being the information or data themselves, which are specifically bound to the medium on which they were initially found.

There are also opinions according to which the criminal offence is without a material object (Streteanu, 2008), because information, data and news cannot be linked to a physical existence, the medium through which they are distributed being just the means of committing the offence. This is also the opinion that is adopted by the author of this article, because the multitude of mediums, through which and the speed at which they are transmitted, by itself, does not directly affect the data, news and information.

In the case of Decision no.14 on 20.03.2020, this was transmitted as an electronic document, and it was spread, including on the news websites, maintaining the form and appearance of an official document.

The subject of the criminal offence

The direct active subject (author to the criminal offence of communicating false information) can be any responsible individual, who knows about the false character of the communicated or spread information. The lawmaker did not condition the quality of the active subject of the criminal offence. The deed in discussion can be committed by one or more persons, in participation. These could be co-authors, instigators or accomplices. Although the active subject is not circumstantiated, it can be remarked that there are specific categories of people that would have it very easy to commit such a criminal offence. For example, people which activate in the field of mass media, or individuals with duties in the public administration in the field of developing and/or keeping the documents. Therefore, particular attention must also be given to the intent when committing an offence (Cioclei et al., 2016).

The active subject in the present case, the individual who had access to the draft of the document from the Technical-Scientific support group for management of highly contagious diseases on the territory of Romania, who disclosed the document to the public, with an official appearance, without any mention of a draft, and even if it was not approved, becomes the active subject. The intent of the person who spread the document cannot be ascertained, but the immediate effects which it produced, in the short period till the official clarification, can be followed. The immediate reaction of the public that received the document through social media platforms was the result of the speed at which information is spread in this media, but also of the high capacity of the public to process the information which they are presented with.

The passive subject

The main passive subject of this criminal offence is the state. There is the possibility of a secondary passive subject, when the data, information or documents refer to a state authority that is prejudiced, maintaining the condition of creating a danger regarding national security. In the analysed case, the National Committee for Special Emergency Situations can be considered a secondary passive subject, as a prejudiced state authority, if the national security was endangered.

The objective aspect

The objective aspect of the criminal offence is constituted from two parts. The lawmaker incriminated first of all the communication of data, information, news or documents that are fake, and secondly their spread.

The difference between the communication and spread is that through communication one aims to directly inform another person or persons in order to obtain the desired results, and through spread one aims to transmit the false information in such a way that it reaches the public, which leads to obtaining the desired results (Ibid.). In both cases, the fulfilment of the following three conditions is necessary: the information must be false, it must endanger the national security, and the perpetrator must know that the spread/communicated pieces of information are false.

In order to verify if the first condition is fulfilled, the notion of *"false information"* needs to be further explored. The Penal Code incriminates the offences of forgery and use of forgeries, in a well determined manner, especially regarding official documents. Thus, defining the notion of *"false documents"*, in the sense of art. 404 Penal Code, can be done with ease. On the other hand, the notions of *"false news, data or information"* are not clearly defined by the lawmaker. In order to better understand these definitions, we need to make an incursion in the lawmaker's thoughts, regarding the concept of *"fake news"*, in the year 2020,

also regarding the fact that it represents a modern phenomenon, which was not so widespread at the moment of the creation of the New Penal Code in 2009. In the National Defence Strategy, suggestively entitled *"Together for a more secure and prosperous Romania in a world marked by new challenges"*, we find at the 8th point of the introduction the fact that: *"The evolutions from the technological domain determines the diversification and growth of the complexity of security risks and threats, like cybernetic attacks, activities specific to the criminal domain (hostile actions/of influence carried out in the public space, disinformation, spread of false/fabricated news etc.), and possibly harmful and destabilising effects of the import of new technologies of civil use within asymmetrical and hybrid actions, generating new security challenges"*. (Romanian Parliament, 2020). Thus, the lawmaker frames the action of spreading false/fabricated news under the concept of disinformation, which is considered to have a harmful effect on national security.

In the European Commission's Plan of action against disinformation, this concept is defined as being a *"series of information that is verifiably false or misleading, which is created in order to obtain an economic gain, or to deliberately mislead the public in order to create a public prejudice. Public prejudice includes threats regarding the democratic processes, but also public assets like the health, the environment or the security of the Union's citizens. Disinformation does not include unintentional errors, satire, parody or news and partisan comments that are clearly identified as such"*. (European Commission, 2018).

In the case analysis regarding Decision no.14 on 20.03.2020, it must be analysed if the content of the document is part of the category of information which may be considered disinformation according to the definition above given. Although the document represented just a draft for internal use only, in the moment it was publicly disclosed through the use of social media, it could be considered a document containing a *"series of information that is verifiably false or misleading"*, because it was not an officially approved document, but it had the appearance of such a document, using the specific format of the decisions which were already adopted till that moment, and also using the distinct marks of the supposed issuing institution. Even the title, *"Decision no. 14 on 20.03.2020"*, denotes the immediate applicability of the measures contained in the document, and the first paragraph can mislead any reader about the official and mandatory character of the document: *"Taking into consideration the increase of infections with SARS-COV 2 at national level, on 20 March 2020, the members of the Technical-Scientific support group for management of highly contagious diseases on the territory of Romania, discussed the measures needed to be taken in order to prevent the spread of infections. The members decided the following: (…)"*. (Gândul, 2020).

Analysing the document from the perspective of its effects, in comparison with the definition given to disinformation by the European Commission, it cannot be appreciated if it was publicly disclosed and spread in order to create an *"economic gain"*, but it certainly had as an effect the misleading of the public, with the potential to create a public prejudice under the form of a threat related to *"the democratic processes and (…) the health, the environment or security of the citizens"* (European Commission, 2018), taking into consideration the fact that the document consisted of a series of drastically restrictive measures which targeted the citizens' freedom of movement, constitutional right, which could be restricted only by law, according to article 25, paragraph 1 from the Romanian Constitution (Romanian Parliament, 2003). Thus, the question arises if this type of document could bring a prejudice to national security. Article 1 from Law 51/1991 regarding the national security of Romania, defines this concept as being, the *"state of legality, balance and social, economic and political stability, necessary for the existence and development of the Romanian state as sovereign, unitary, independent and indivisible, maintaining the lawful order, and also the climate of unrestricted exercise of rights, freedoms and obligations of citizens, according to the democratic principles and norms, established through the Constitution"*. (Romanian Parliament, 2014). Taking into consideration the contents of the previously mentioned article, we can assess that through the creation, in the eyes of the citizens, of an apparent restriction of rights that are guaranteed by the Constitution, a prejudice is created to the Romanian state, affecting the "state of legality, balance" and also affecting the *"climate of unrestricted exercise of rights, freedoms (…) according to the democratic principles (…) established through the constitution"*. As a result, the sole creation of a perception in the citizens' eyes, through misleading, that would affect the previously mentioned principles, could be considered a threat to national security.

The third requirement necessary for the fulfilment of the objective side requirements of the criminal offence is decisive, according to the Romanian Constitutional Court: *"the action of communicating or spreading news, data, information or documents become relevant from a penal point of view, only under the condition that the perpetrator knew about their unreal character, at the moment when the crime was committed. This means that any doubt about the authenticity of the communicated or spread information makes the criminal offence's constitutive elements unable to be fulfilled, producing the same effect as the cause of no liability in case of error. This situation derogates from the normal rule in this field (according to which error must not be mistaken for doubt, the latter meaning that the perpetrator is aware that he cannot fairly represent the reality in which he should not act, and, if he does act – even though he is aware that he is unsure of the reality -, will be criminally responsible for the deed, because he accepted the socially dangerous result, thus acting with indirect intent). In other words, only the subject that knows about the false character of the spread data, information or communication is criminally liable, but not the person that has doubt about their value of truth, even though, from an objective point of view they are unreal. Thus, in the legislative frame we find a transposition of an older orientation, of doctrine and case law, that stated that the criminal law does not sanction the communication or spread of data and information just for the simple reason that their authenticity was not confirmed, but it takes into consideration the false data or information, and also the false documents, thus the perpetrator cannot be made criminally liable for the disclosure or data, information or documents with about whose authenticity he was unable to know about"* (Decision no. 273/2000). Although the previously cited decision refers to the provisions of the article from the old penal code, the prosecution of the discussed deed can be found under the same form, the judgement of the Constitutional Court of Romania finding its applicability in the case of the new provision too. Regarding the analysed case, it remains for the criminal prosecution bodies to determine if the person who disclosed and spread *"Decision no.14 on 20.03.2020"*, had doubts about the value of truth of the document's contents, although it is hard to accept the fact that the disclosure, in good conscience, of a document that was not subjected to the process of approval, represents a version in which the perpetrator does not know about the unreal character of the disclosed information.

The immediate consequence of the criminal offence stated in article 404 Penal Code is the creation of a perilous state that affects national security, and regarding the causality link, a direct relationship between the deed of disclosing false information and the state of peril for the national security is mandatory. Both estimating the impact of the deed against national security and the direct relationship with the created state remain to be determined by the bodies with responsibilities in this field.

The subjective aspect

Regarding the subjective aspect, the lawmaker only takes into consideration the form of offence with intent. This is the reason why a more detailed analysis of the way in which the author of the deed perceived the disclosed information, according to the decision of the Romanian Constitutional Court, previously mentioned. Also, from the doctrine, it can be noted that if *"the author has doubts regarding to the character of presented information, but chooses to expose them do the public opinion, no matter how irresponsible or devoid of professional deontology would be his activity, especially when he is a journalist, he cannot be held criminally responsible"*. (Cioclei et al.).

Forms of the criminal offence and sanctions

For the communication of false information, the lawmaker sanctions only the criminal offence consumed under the form of the effective realisation of the communication or spread of false information, having the requirement of creating a state of peril for the national security. An important fact to remark here is that the consumption of the criminal offence is not conditioned by the effective reception of information by the targeted public, if the simple spread of this information can create prejudice to national security. Also, according to article 412, paragraph 2 from the Penal Code, the attempt is not punishable (Law 286/2009).

The criminal offence of communicating false information is punished with prison from one to five years, no matter the way of committing the criminal offence.

CONCLUSIONS

Taking into consideration the premise from which this research has started, analysing, from the perspective of the Penal Code, a part of the phenomenon spread on social networks, which is in continuous development, known under the name of *"fake news"*, and realising a real parallel through the use of the case of *"Decision no. 14 on 20.03.2020"*, some conclusions can be drawn regarding the way in which article 404 from the Penal Code, regarding the criminal offence of communicating false information, finds its specific applicability over the documents disclosed and/or spread using the online medium.

The constitutive elements of the criminal offence stated by article 404 in the Penal Code can also be easily found in cases in which the false information communicated aims to misinform the general population, and the fact that we find this concept defined by the European Commission in the *"Action Plan against Disinformation"*, with similarity to the way in which the Romanian lawmaker understands the concept of communicating false information, only strengthens the conviction that the applicability of the discussed criminal offence must be extended in order to also grasp the communication made through social networks, especially that some of them are already considered public domain (Decision 4546/2016). Moreover, the recognition on the part of the Romanian lawmaker of the danger that disinformation represents, under the different forms that it takes, for the national security, in a legislative act such as the country's National Defence Strategy for the period 2020-2024, shows the necessity of revising concepts that are applicable in cases similar to that of *"Decision no.14 on 20.03.2020"*, and also strengthening the legal instruments in order to incriminate such deeds.

As such, for the improvement of the legal framework that finds application in the analysed cases, a Lex ferenda proposition can be made, by introducing a new paragraph in the content of article 404 from the Penal Code: *"(2) With the same punishment are sanctioned the offences mentioned in paragraph (1), committed with the aim to misinform the general population in order to create a situation that brings peril to national security"*, thus facilitating the incrimination in cases similar to that of *"Decision no.14 on 20.03.2020"* for the effects produced on the target audience, and not only by sanctioning the criminal offence according to article 304 Penal Code regarding the offence of disclosing secret or classified information.

BIBLIOGRAPHY:

1. Cioclei, V., Nedelcu, I., Manea, T., Lefterache, L. & Kuglay, I., Bodoroncea, G.,Vasile, F.-M. (2016). *Codul Penal. Comentariu pe articole*. 2nd ed. București: C.H. Beck.
2. Dobrinoiu, V., Pascu, I., Hotca, M.A., Chis, I., Grounescu, M., Păun, C., Sinescu, M.C. (2014). *Noul Cod Penal comentat*. Partea specială. IInd edition. București: Universul Juridic.
3. Streteanu, F. (2008). *Tratat de Drept Penal*. Partea generală, vol. I. București: C.H. Beck.
4. European Commission. (2018). Action Plan against Disinformation, https://eur-lex.europa.eu/legal-content/RO/TXT/?qid=1547476841326&uri=CELEX:52018JC0036, retrieved on 23 September 2020.
5. Decizia nr. 273/2000 referitoare la excepția de neconstituționalitate a dispozițiilor art. 168 din Codul Penal (Curtea Constituțională a României, 28.02.2001).
6. Decizia nr. 4546 (Înalta Curte de Casație și Justiție – Secția contencios administrativ și fiscal, 27.11.2016).
7. Decret nr. 195 din 16 martie 2020 – privind instituirea stării de urgență pe teritoriul României. Monitorul Oficial al României, no. 212.
8. Decret nr. 240 din 14 aprilie 2020 – privind prelungirea stării de urgență pe teritoriul României. Monitorul Oficial al României, no. 311.
9. Gândul. (2020). Hotărârea nr. 14 din 20.03.2020 – BREAKING NEWS! România, în "arest la domiciliu"?!, https://www.gandul.ro/stiri/ultima-ora-draft-documentul-de-care-am-putea-avea-nevoie-pentru-a-parasi-domiciliul-19406589, retrieved on 23 September 2020.
10. Grupul de Comunicare Strategică. (2020). Precizare Grup Comunicare Strategică, https://www.mai.gov.ro/precizare-grup-comunicare-strategica/, retrieved on 23 September 2020.
11. Legea 286/2009 – privind Codul Penal, cu modificările și completările ulterioare. (2009). Monitorul oficial al României, no. 510.
12. Parlamentul României. (2003). Constituția României (republished in 2003). Monitorul Oficial, no. 767.
13. Parlamentul României. (2014). Legea 51/1991 privind securitatea națională a României – republicată, cu modificările și completările ulterioare. Monitorul Oficial, no.190.
14. Parlamentul României. (2020). Hotărârea nr. 22/2020 privind aprobarea Strategiei de Apărare a Țării pentru perioada 2020-2024. Monitorul Oficial, no. 574.

ANALYSIS OF THE MAIN INTERNAL COMPONENTS OF THE BLACK SEA SECURITY SYSTEM – THE MAIN CHARACTERISTICS OF THE NATIONAL SECURITY OF ROMANIA THROUGHOUT THE 20TH CENTURY –

Consul General Marius-Sorin MICLEA, PhD

Embassy of Romania in the Republic of Cyprus

Internally, immediately after the end of the Cold War, the Black Sea region appears configured as an unstable region, on whose territory economically weakened states were in competition, affected by a pandemic corruption that was eroding the basis of newly established democratic political regimes, descendants of totalitarian regimes that had recently succumbed. Most of the vigour of these states was consumed in a series of sterile political controversies, in a fragile legislative framework, which had replaced the ossified structures of the former so-called popular democracies. The parliaments of these states were also, in turn, wired by corruption and characterised by a lack of interest in the real and, especially, the serious problems of the population. Despite these realities, the population was overwhelmingly in favour of integrating those states into NATO and the European Union.

The former Soviet republics, Georgia, Ukraine and Armenia, also began to show, in turn, the germs of a European orientation, timid, indeed, but remaining dependent upon residual communist reminiscences specific to the mentality perverted by the totalitarian regime. In these circumstances, it seemed certain that at least another generation would have to pass for these states to change their mindsets deeply rooted in communist reality.

Keywords: community space; Black Sea; communism; Warsaw Treaty Organisation; interwar period;

INTRODUCTION

Due to its geographical position, the Wider Black Sea Region covers a territory that includes many states, a puzzle of Western, Islamic and Orthodox civilisations. Romania's position in this context raises the issue of both its and the other states framing in a regional archetype from a geographical and civilisational point of view. As a method of analysis/research, when establishing the position of a state, we will analyse the architecture of the present forces and their activities on the geopolitical scene, taking in consideration the major objectives and targets of the region. The identification and analysis of state geostrategies, of the tools through which states are involved in order to achieve the proposed goals are useful methods, necessary to complete this analysis.

Geopolitics addresses the goals of cooperation and the elimination of tensions between states, as well as the use of force to conquer military supremacy. It encompasses the concerns of actors on the international stage, regardless of who they are, government officials, diplomats or NGOs. Public opinion is extremely sensitive when it comes to the protagonists' plans that reflect the heterogeneity of space and natural, historical and religious conditions. From this point of view, the post-Cold War international context was extremely favourable for Romania, because it offered the possibility to play a very important role, that of a bridge between East and West, as well as the turntable of intra-European connections between the old continent and the neighbouring regions.

The problem of establishing Romania's position could be determined, to a large extent, taking into account the interests of the great powers in the region, as well as their impact on the region. The hierarchy of the states of the region, the predominant cultural and spiritual values and the security approach of the issue by each state could complete this picture. In the extremely tense period following the collapse of communism, there was a clear process of polarisation between political, military and economic powers and, from another perspective, between world, continental, regional and sub-regional powers. There were also states that were too weak to make their views known on the process of ongoing international events.

Contextualising the above considerations, we still have to analyse to what extent the zonal actors really wanted to transform the security environment, but, especially, to what extent and at what cost was the United States of America willing to counteract Russia's interests in the region. Other topics of utmost importance also remain open to our analysis, such as the manner in which the European Union wants to involve itself in the region and, especially, what is the extent of the geographical areas in which Russia wants to restore its old empire. Will this be limited only to the former union republics or will it give way to the pan-Slavic barrier and proceed to the conquest of new territories belonging to independent states which, from an administrative point of view, were never part of the former Soviet Union?

GENERAL CONSIDERATIONS ON THE POSITION HELD BY ROMANIA IN THE REGION AFTER THE END OF THE COLD WAR

Making an analysis of Romania's position on the international stage, we conclude that its role must be approached in terms of its sensitive position in the region. In its double capacity as NATO and EU member state, it fulfils a defensive mission for Europe. To the same extent, Romania also fulfils a defence role for the Black Sea region, through its defence and international policies. Romania has thus become a regional exporter of security and stability[1]. Romania's integration into European organisations will transform the eastern Black Sea coast into an area controlled by the Western allies. Thus, the entire process of European integration ensures NATO's rapid and efficient access to the Middle East, and the entire region will move from the Kremlin's orbit into the sphere of Western influence.

The Euro-Atlantic area is a European institutional area that is neither cultural, nor ethnic, nor geographical. The American idea of creating a free and united Europe practically means projecting the Western framework (represented by NATO and the EU) to the East. The eastward advance of the western borders structured the space of the Wider Black Sea Region on two axes, representing two connotations, one geopolitical (economic and strategic) and one political, referring to the East-West and North-South axes.

[1] According to *Romania's national security strategy* of 2006, *"national security is ensured through its own forces and through cooperation with allies and partners, in accordance with its own strategies and strategic concepts of the Alliance and the strategy of the European Union. It provides for the harmonisation of national efforts with international commitments and the identification of ways of working to prevent and counteract threats in a timely manner. Efforts are also aimed at promoting democracy, peace and stability in the neighbouring region and in areas of strategic interest, reducing vulnerabilities, building adequate national capacities, and profoundly transforming security institutions".* (A.N.).

The East-West axis includes the Caucasus and the Caspian region, its much-needed energy resources for the West, and the Black Sea extends this axis.

The North-South axis includes Russia, Armenia and Iran. At the crossroads of these axes are Azerbaijan (a key security region), Georgia, and Armenia. The Asian energy corridor is a rather unsafe access route in the region, located in northern Transnistria, passing through Odessa and Sukhumi. The reason for the fragility of this access route is given by the frozen conflicts that intensify the insecurity of the region and that must be resolved before reaching the serious situation of their expansion and spread in states where the problems that triggered them do not exist. Hypothetically, Romania is framed by four geostrategic sub-regions of Central and Eastern Europe. The first sub-region includes the Central European states, Poland, Germany, Austria, Czech Republic, Slovakia, Hungary, and the Baltic States, the sub-region being positioned in the western part of Romania.

The second region, that of Southeast Europe, consists of Albania, Bosnia-Herzegovina, Bulgaria, Greece, Kosovo, North Macedonia, Montenegro, Serbia, Slovenia, Turkey. The Black Sea riparian basin consists of Romania, Bulgaria, Ukraine, Moldova (it is a state without a seacoast, but the port of Giurgiuleşti gives it access to the Black Sea), Russia, Turkey and Georgia.

It is useful for our analysis to take into account the specific, geographical, spiritual, economic and historical particularities of the states positioned in the four areas. Certainly, the significant geopolitical events of the Black Sea region (evolutions, involutions, as well as the full range of events that define the Eastern strategic climate) are the result of the advance of the Euro-Atlantic border towards Asia. This phenomenon is part of the global geopolitical evolution, as a result of changes in the poles of power worldwide. However, the problems in Eastern Europe are the result of the indecision of Western European bodies to set a sufficiently large border to include the countries and nations wishing to be part of the Western security system in the sphere of Western influence.

From a geographical point of view, the Carpathian Mountains and the Danube are landforms that, at first sight, represent a geographical border between Europe and Romania. However, we consider, these natural obstacles are not major elements that could create the illusion that Romania would be part of a geographical area other than the European one (Huntington, 1997, pp. 145-146)[2]. Therefore, from this point of view, Romania can be placed in the first region, which includes the states of Central Europe, along with Germany, Hungary, Poland, Austria Czech Republic, Slovakia and Baltic States. From a historical perspective, there is a long common past with these states over the centuries. The communist experience turned Poland, Hungary, the former Czechoslovakia, the former German Democratic Republic, Romania into Soviet satellites. An apparent block solidarity contributed to the rapprochement of these states during the Cold War, even if it was a façade solidarity, imposed by the canons of proletarian internationalism. That is why, after the fall of communism, this false rapprochement disappeared, and the states became seen by the West as serious competitors.

In the period immediately following the disappearance of communism (a situation perpetuated to the present day), the economic factor is what separates Romania in a decisive way from the other states that escaped from the yoke of Moscow[3]. Led by the existence of an immature political class, affected by the highest rate of corruption in the community, by an increased rate of emigration, Romania certainly did not meet the expectations of this group of states in the period immediately following the great geopolitical changes after the fall of communism. If we add to the equation the issue of Romania's belonging to Orthodoxy, given that the other states are Catholic, we find, at the end of this summary analysis, that Romania does not have enough affinities and elements of connection with Central European states, as they were configured.

[2] According to Samuel Huntington, Romania is considered a non-European state, due to the great historical line that separates the Western Christian peoples from the Orthodox and Muslim peoples. The fault line, according to the same author, divides Romania into two, Catholic Transylvania on the one hand, and the old Kingdom on the other, together with Moldova and Dobruja, which are predominantly Orthodox. A few remarks are required, however. First of all, today's Euro-Atlantic Europe is an institutional space, but not a civilisational or cultural one. In any case, Europe's institutional borders do not coincide with geographical, cultural and civilisational ones. On the other hand, Transylvania is a region of Romania, which is a sovereign, independent, national, unitary and indivisible state, according to the Constitution. The Hungarian or Catholic elements do not exceed the figure of 2.4 million inhabitants throughout the country, which includes 21 million inhabitants. Even in Transylvania, which is predominantly Orthodox, the Hungarian element is a minority. In these cases, Huntington's statements raise questions about the true political purposes of this division. Being a Latin state, belonging to Western civilisation, and identifying with Western cultural and spiritual values, it represents a happy ambivalence of Romania, demonstrating the permanence of this Latin country in a Slavic sea, at the eastern borders of Europe. (A.N.)

[3] The process of integrating Romania and Bulgaria into the European Union placed the two countries in the first place in the top of poverty at EU level. The first criterion of this ranking is the Gross Domestic Product (GDP). In Romania and Bulgaria, it represents only 34% of the level of European countries. These states rank first in terms of unemployment, mortality, and last in terms of fertility, birth rate, number of people with higher education. Romania, together with Bulgaria, ranks last in terms of living standards, with 37% of the average of the community states. (The data was obtained from the journal *"Guardian"*, dated 03.01.2007, and is the result of a study prepared by the National Commission for Long-Term Forecasts) (A.N.).

Regarding the states belonging to the second group, Hungary's attitude towards Romania has been repeatedly nuanced, and it has never overlooked the territorial losses it suffered as a result of the entry into force of the provisions of the Treaty of Trianon, by which Transylvania, the cradle of the Romanian people, was returned to its rightful owner. After 1989, Hungary chose its own path to the West, being also one of the artisans of the Visegrád Treaty, to which Romania was not invited.

As for the relations between Romania, and the other central European states mentioned above, we are very far from finding linguistic, cultural and historical rapprochements. From an economic point of view, the European states have a major economic ascendancy over Romania. Its explanation lies in the fact that the communist regime did not prove to be as harsh as it proved to be in Romania. It allowed the basis of a market society/economy, along with an economy/nationalised and planned according to the socialist model. Although it is not part of the region, Yugoslavia, another former socialist confederation located in Eastern Europe, can be an example in this regard. It is well known that Marshal Tito encouraged his own citizens to work across the border, an initiative that pumped added value into the Yugoslav economy from the money of Yugoslav workers across borders.

After the euphoria aroused by the courage to face the communist regime in December 1989, Romania was placed, by the Western media, through an intense press campaign, at the top of the communist states, benefiting from a huge capital of sympathy and solidarity. Later, however, as elements that would highlight the dark and somewhat blackened parts of the Romanian revolution began to emerge, this capital of sympathy gradually faded as the truth came to light. If we add to these causes the intolerance and violence that characterised the ethnic conflicts in Târgu-Mureș, the series of miners' rampages, the decline of the economy, we can notice that Romania's laudable intentions to join were deeply discredited, and the integration process proved to be much delayed.

From this perspective, immediately after the fall of communism in Europe, it became clear that both Romania's long common past with these states and the suffering they endured together during cohabitation under the umbrella of the Warsaw Pact were of little value in the new zonal security configuration, and Romania's economic decline was one of the major reasons for its removal from the states of this last group of Central Europe.

Starting with 2000, the year Vladimir Putin took power, it became clear that the great hegemon of the East, once the geostrategic *"attractor"* of the socialist member states of the sanitary cordon deployed in front of the Western states, began to tread the path of restoring its imperial status. Russia's path to the goal is that of geographical expansion in all directions. If during the Tsarist Empire, this desideratum was hidden under the coattail of *"Pan-Slavism"*, in the era of the Soviet Union under that of the *"export of the proletarian revolution"*, in the 21st century, Dughin's Eurasianism[4] is for Putin the ferment necessary to initiate his policy of conquest, the first result of which was the annexation of Crimea.

ROMANIA – KEY STATE AND PLAYER IN THE WIDER BLACK SEA REGION. THE MAIN FEATURES OF ROMANIA'S NATIONAL SECURITY THROUGHOUT THE 20TH CENTURY

Romania is, without a doubt, one of the main geostrategic actors in the region. Due to its geographical location west of the Black Sea, through its demographic, military and economic potential, Romania is able to position itself in the group of powers bordering the Black Sea, such as Bulgaria, Ukraine, Moldova, Russia, Georgia, Armenia and Turkey. From a cultural point of view, Romania is the only Latin state in the area, but the beneficiary of a dual identity, both Western and Eastern[5]. As mentioned, the country is located at a crossroads of the region, being, throughout history, the first European bastion with the mission to block the advance of migrating nations to the west. Thus, Romania's security values are not recent at all, having their roots in Antiquity. Bivalent ancestry, western and eastern, is an asset for Romania, but also for the West. Trained in Western schools, Romania's top leaders have contributed to the transformation and development of modern Romania, knowing how to combine the Western spirit with the traditions of Eastern civilisation, in a way capable of allowing social progress in this part of the world.

National security has always concerned the political class of modern Romania. Unfortunately, until the end of the Cold War, national debates in this area were compromised by a detrimental policy inherent in totalitarian regimes. Throughout history, Romania has had to reshape its national strategy according to the different regional hegemonies that have operated in this part of the world. These changes have been driven by major changes in the global security environment that have affected the regional security framework.

The preliminary period of the Great War was marked by a dangerous underestimation of the national security policy. A political class subservient to clan interests often placed its own interests above national interests. Romania was, at that time, in the situation of a dismembered state, having large portions of territory under Russian (Bessarabia and Northern Bukovina), Hungarian (much of Transylvania) and Bulgarian (Southern Dobruja) occupation. In 1914, Romania had to endure the pressures of the Great Powers, in order to enter the war on the side of one camp or another. However, following its cultural and historical affinities, but especially as a result of the promises from France that it would support, after the war, the unification of Romanians from all provinces, Romania opted for the Allies camp to the detriment of that of the Central Powers. The decision was a wise one, considering that, after the war, the country found itself in the camp of the *"winners"*, and the historical process ended with the Great Unification on 1 December 1918.

The interwar period marked a stage of important economic growth for a unified Greater Romania, thanks to the national consensus and the euphoria after the First World War. In the interwar period, the isolation on the international stage of Romania's old allies (France and Great Britain) generated great threats against Romania, which saw itself alone in front of two great enemies: the Nazi Germany and the Soviet Union. Thus, in 1940, with the help of the two great enemies, as well as of two neighbouring states, the great territorial amputations happened through which Romania, defenceless, ceded Bessarabia and Northern Bukovina to the Soviet Union, the part of northern Transylvania to Hungary and the Southern Dobruja to Bulgaria.

In 1940, Romania opted for a conjunctural alliance with Hitler's Germany, renouncing the guarantees of more and more abandoned Western powers

[4] Alexander Dughin (born 7 January 1962), Russian political analyst and strategist with close ties to Kremlin power circles and Russian military circles. His father was a GRU general. He is a graduate of the Moscow Aviation Institute, but did not get his diploma. Organiser of the National Bolshevik Party, the National Bolshevik Front and the Eurasia Party. Author of over 30 books, among them, *Foundations of Geopolitics* and *The Fourth Political Theory*. Promoter of the theory of neo-Eurasianism.Source: https://en.wikipedia.org/wiki/Aleksandr_Dugin, retrieved on 28.10.2020.

[5] According to French professor Catherine Durandin, *"there is no recent history of Romania in French. After December 1989, I saw an audience mad with images of violence, those of the Revolution of December 1989, Romania belonging to the oriental space, that of orthodoxy, that of the history of the periphery of the Russian space, then Soviet. It belongs to a Western European field, which has its origins in the Springtime of the Peoples of 1848, as well as the western attitude of Romania, that of non-intervention, in August 1968, during the invasion of Czechoslovakia by Warsaw Pact troops. A dismembered state, obsessed with an identity crisis, Romania had lived and survived all the hurricanes and storms throughout history, claiming to have invented a specificity outside of history. It is a state marked by a duality of history, being pushed, throughout history, both to the west and to the east. Today, the same country, which Westerners tend to blame for being a liar, opts globally for some kind of modernity that pushes it toward Western Europe*, on the website http://www.franceculture.com/oeuvre-histoire-de-la-nation-roumaine-de-catherine-durandin.html, retrieved on 28.03.2020.

on the international stage, a decision that could not prevent territorial amputations. The decision to fight alongside the Axis powers turned out to be bad for the country because, at the end of the war, it was on the side of the defeated. Although it regained Transylvania through the Paris Peace Conference, Bessarabia, Northern Bukovina, as well as the Southern Dobruja remained lost, it seems forever, for Romania. The return of Transylvania to the Motherland proved to be the beginning of a long period of territorial disputes between Romania and Hungary. Although the communist ideology apparently froze the subject of Romanian-Hungarian confrontations, there was never any silence on this subject, and the end of the Cold War reopened this old wound, a subject of dispute between the two neighbouring states.

The establishment of communism in Romania sanctioned the confinement of the country in the *"camp of the states of popular democracy"*. Officially, the country's independence, sovereignty and integrity were guaranteed by the new *"popular"* Romanian armed forces and by its faithful ally, the Soviet Union. The process of communisation of the Romanian Armed Forces brought the cadres of the old Royal Army into a dramatic situation, many of them being massively placed in reserve and thrown into the sinister communist prison by the *apparatchiks* and politruks of the new communist army. The communised Romanian armed forces represented, themselves, the greatest risk to Romania's national security, because, in the event of a Soviet invasion, in the early years of the establishment of communism, no Romanian military would have opposed the invading troops[6]. The equipment, training and procurement of the Romanian Armed Forces left much to be desired, while military commanders were trained in large numbers in Soviet military academies, where most of them were recruited by the GRU (Main Intelligence Directorate). Consequently, the feeling of belonging to the national values of the Romanian Armed forces was almost non-existent in the society of that period.

[6] Obviously, our reasoning refers to the first years of the communisation of the Romanian Armed Forces, a period when it was effectively reconciled with the soldiers of the *"Horia, Cloșca and Crișan"* and *"Tudor Vladimirescu"* Divisions, the famous large units formed by Romanian volunteers, indoctrinated with communist ideology after their fall into captivity in the USSR. To these elements are added the political officers (apparatchiks and politruks) in charge of indoctrinating the military personnel. This situation radically changed after the takeover of power by Nicolae Ceaușescu, a national leader who, at that time, moved away from the Russians through his nationalist policy.(A.N.)

The Warsaw Pact enacted the presence of Soviet troops in the national territories of the communist member states. Romania's national security was subordinated to the doctrinal and politico-military concepts of the Soviet Union. The Romanian communist regime, enslaved to the Kremlin, proclaimed the supremacy of communist ideology, Soviet military strategy and doctrine. The development of a national defence strategy as well as a national defence doctrine were impossible to achieve at that time. The withdrawal of Soviet troops from Romania in 1958 and the takeover of power by Nicolae Ceaușescu in 1965 completely changed the data of the problem. On that occasion, the nationalist-communist zeal replaced proletarian internationalism, and this changed Romania's image in the Treaty, from a faithful and obedient ally of Moscow to a *"rebel"*, whose marginalisation in decision-making at the level of the organisation became more and more necessary, as Bucharest's attitude proved more and more critical towards the Pact.

The essential component of the new Romanian foreign policy adopted by Nicolae Ceaușescu consisted in the emancipation of Romania from the political tutelage of the Soviet Union. The Romanian leader considered that it was essential for Romania to create its own path of development, sanctioning as fundamental principles of the Romanian foreign policy the mutual respect and equality between states, within the international relations. On that occasion, a new defence doctrine was developed, and new and promising perspectives opened up for the national defence industry, with the ultimate goal of total elimination of Soviet imports of equipment and weapons. However, the practical application of that desideratum proved to be extremely difficult, due to the complexity of the activity, the high standards to be observed in military production, as well as the lack of a skilled labour force in the field.

The decade of the '70s and '80s marked an important step for Romania's national security. The concept of *"battle of entire people"* was transposed by the communist regime in a scientific structural framework for the first time in the history of Romania. A new national military doctrine was developed. Thus, practically, every member of the Romanian society, every citizen of the Socialist Republic of Romania was obliged to participate in the effort to defend the socialist state since an extremely young age. For the first time, Romanian cities were spoken of as *"cities of work and defence of all people"*. The participation of all workers, peasants and intellectuals in the paramilitary formations of the Patriotic Guards was mandatory, becoming a mass phenomenon. The children of socialist Romania were enrolled from the age of five in the political organisations of the *"Fatherland's Falcons"*, nurseries of pioneer organisations and communist youth. Thus, the militarisation of Romania had become total.

CONCLUSIONS

Although Romania was a full member of the Warsaw Pact, defence plans were drawn up by communist leaders in a multidirectional manner, in compliance with the new national doctrine according to which a possible attack on Romania could occur from any geographical point, including from the Warsaw Pact allies. This proved to be a unique case among the members of the Treaty. The official doctrine of the latter, drawn up by the Soviet Union, provided that an attack on socialist states could only take place on the part of NATO member states, predominantly the United States of America, considered the supreme enemy, not on the part of the socialists, but this fact was refuted by reality[7]. As a result, the war plans of the private voluntary organisations (WTO)[8] were designed taking into account the foreseeable directions of a massive offensive launched by NATO against the socialist prison. Of course, each member state of the Warsaw Pact was assigned specific tasks in the case of overall missions.

Given the national peculiarities of Romania (its geostrategic position) as the only socialist state surrounded only by socialist states, its obsolete military equipment, as well as its reputation as a *"rebel"* within the organisation, its role in the defence device was of the second rank, the Romanian troops being destined to perform missions within the second echelon of the military device, acting with small numbers.

This strategic duality of Romania (the existence of a defensive national doctrine in which the enemy could also be a socialist state, as well as its role of power of the second rank within the Warsaw Pact) made Romania a particular case in the region. From the same perspective, the inconstancy and duplicity of the Romanian communist leaders weakened Romania's overall position during the Cold War. Bucharest could no longer rely on the solidarity of the other socialist states in the same camp, and for them, Romania was an unfaithful, unstable, recalcitrant ally, which asked awkward questions at every WTO meeting, with obvious outbursts of nationalism. At the end of the communist era, Romania represented, for the Westerners, a closed country, totally isolated from the international community, led by a tyrannical regime. For the other socialist leaders of the pre-transition to capitalism period, Ceaușescu was the *"scapegoat"* for the deplorable situation in Romania before the events of December 1989, which put an end to that regime. Although the Romanian Revolution managed to overthrow a criminal regime, on the other hand, it created a breach in Romania's national security.

[7] See the cases of the uprising in the German Democratic Republic (1953), the uprising in Hungary (1956) and the case of the invasion of Czechoslovakia by the socialist states (except Romania) in 1968 (A.N.).

[8] Abbreviation for Warsaw Treaty Organisation.

BIBLIOGRAPHICAL REFERENCES:

1. Huntington, S. (1997). *Ciocnirea civilizațiilor*. Editura Antet.
2. *Strategia de securitate națională a României – România Europeană, România Euro-Atlantică: pentru o viaţă mai bună într-o ţară democratică, mai sigură şi prosperă*. (2006). București.
3. http://www.franceculture.com/oeuvre-histoire-de-la-nation-roumaine-de-catherine-durandin.html, retrieved on 11 August 2020.

SECURITY'S MULTIDIMENSIONALITY – SOCIETAL SECURITY IN THE AGE OF INFORMATION TECHNOLOGY –

Major Laurențiu-Paul MÂNDRAȘ, PhD Student

Defence Intelligence Training Centre, Bucharest

Traditionally, security has been associated with the military field, and setting national interests, triggering war and settling for peace have been the responsibility of the state, an exclusive actor in international relations. Starting in the mid-20th century, security studies have extended the dimension of security to its objective side, mainly military, related to the existence of a threat, and its subjective, societal side, related to the perceptions of society. The modern vision of security has enhanced these two sides, and the European Security School in Copenhagen has conceptualised the societal society, debating on the reduced role of the state and increased role of society in security, manifested in five key areas – military, political, economic, societal and environmental, security being assimilated with the social mechanism. In this contemporary context, the explosive digitization of information and its effects on security and society – globalisation, artificial intelligence, internet, automation, social networks, social engineering, data mining, fake news, cyberwar, cyber psychology – make military superiority inadequate for ensuring peace and security in the 21st century. Therefore, may we assess information technology as the new "nuclear bomb" of the 21st century? Is information technology a new field or a feature of societal security?

Keywords: societal security; society; information technology; threats; civil society;

INTRODUCTION

Security is a social phenomenon, and precisely because of its complex nature, it has always aroused intense debates at national and international levels, both within scientific, political, public or even economic communities.

Attempts to define security are multiple and varied, and they are all connected with how security relates to the components and characteristics that define it, in terms of the degree of adequacy to the objective reality related to which it is identified, the values, the state and society ideologies, ethics, morals or form of religious organisation.

OBJECTIVE AND SUBJECTIVE COMPONENTS OF SECURITY

Considering the spirit of the conclusions generated by the security scholars, a good understanding of security, especially of contemporary security, must take into account a triple hypostasis, regarding the objective and subjective characteristics of the phenomenon. Thus, *objective reality, reality constructed through discourse and security policy and strategy* (Hlihor, 2008, p. 37) are basic characteristics of security. It could be interesting to see why.

Security as an objective reality is manifested especially at the national-cultural state level, and it is related to the interaction between different types of security actors, like the state, the individual and the social group, and the perception constructed by these actors through reflecting the real processes and phenomena that occur within societies or within the international environment.

The mental reflection of security highlights its subjective dimension, as *objective security is subjectivized*, which is manifested at the emotional states created at individual or collective level and in the way they are materialised through human behaviours, including their implications at the state level.

From the *objective* perspective, the goal of security lies in achieving a climate of peace and comfort, and the state is the main actor that takes the measures it deems necessary to ensure its existence, freedom of action and development, and peace, freedom and prosperity of its citizens. The ultimate goal of objective security is peace and defence against any perceived threats, including removing the negative effects such as fear, apprehension, anxiety or panic.

Security as a reality constructed through discourse is a type of security specific to international relations, due to the systemic and anarchic characteristics of the international environment, and peace and war are the main forms of its manifestation (Kissinger, 2002, p. 14). Even though peace is the main desideratum of global society, different forms of war and feelings of frustration, hatred and fear persist in today's societies.

The perception of the factors that affect security has a heterogeneous character, and security as a phenomenon cannot be dissociated from its very opposite, insecurity. Consequently, the international security environment can be analysed only from the perspective of the existence of the security-insecurity binomial, necessary precisely because there is no absolute security that is identical throughout humanity, and, most often, the security of some states or societies generates the insecurity of other states or societies.

The discourse on security is specific to both political and civil society environments, and it includes a number of specific elements, such as security theories used to interpret and analyse security events and processes, security representations, especially those involved in the process of development of security policies, and, last but not least, the perception of security, especially of politicians with responsibilities in this field, who ultimately set and approve security policies (Deutsch, 2006, pp. 4-7).

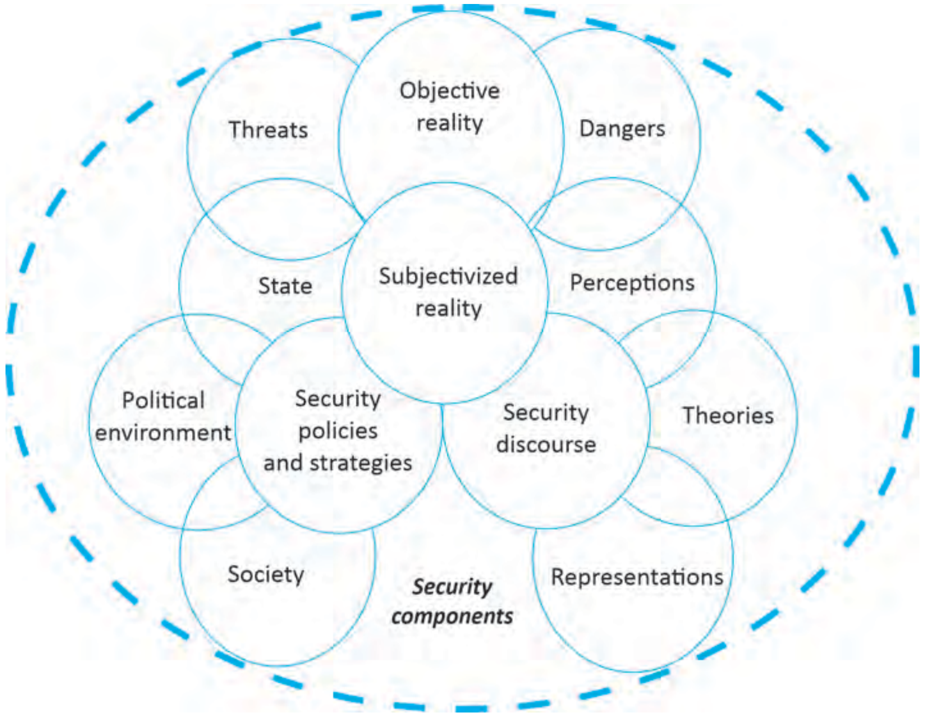


Figure no. 1: Objective and subjective components of security

Given the above explanations, it is easy to understand the impact of objective and constructed through discourse reality, and how security is formed through security policies and strategies interpreted as specific means for international actors, especially states, to understand, to act for and to defend their security interests. This model of action encompasses the threats and dangers perceived against the state or societal existence in space and time, the values assumed, the freedom of action and the capacity to develop and ensure prosperity.

Thus, security policies (Bușe, Hlihor, 2004, pp. 117-126) are influenced by the potential power, understood as military, diplomatic, economic and symbolic power, and the type of power manifested in the international environment, the national policies promoted by the state, the political ideologies and the nature of the political regime, the value system, the historical traditions, the specific mentalities of the communities of reaction to dangers and threats of any kind.

MILITARY, SOCIETAL AND HUMAN SECURITY

Scholars in international relations, security and geopolitics are constantly striving to research and understand the phenomenon of security, in order to create a theoretical and practical framework through which to define security and identify solutions to security problems. As a result, the security domain has been reserved a multitude of theories and meanings through which security is approached unilaterally or multidisciplinary, by relating to the extrinsic and intrinsic reality it belongs to.

Historically, the international system of states, as it is known even today, has its origins in Europe and resulted from the peace treaties of 1648, known as the Peace of Westphalia, which led to the dissolution of the Habsburg Empire, undermining the political authority of the Catholic Church and the creation of nation-states, based on national sovereignty and the fundamental right of these states for political self-determination.

The genesis and development of nation-states have generated a *school of realistic security theory*, already traditional, which argues that states are the main actors in international architecture, and security is the process by which they maintain their sovereignty in the anarchic conditions of the security environment. By defending sovereignty, the followers of the realistic school understand security as the *capacity of the state to defend its territorial integrity, the people, the institutions and the values from any external aggression* (Popescu, 2014, p. 8).

Thus, the state's military security is the study field on which realism is focused, as it argues the fact that the military force is the one and only that ensures states' national defence against other state enemies and the achievement of peace.

Realistic security studies perceive states from the perspective of their fear of war and their military ability to secure or achieve peace, focusing on two main dimensions, namely avoiding domestic or international anarchy and countering possible military attacks by other states.

From a realistic perspective, state security is confused with national security, and its practical achievement depends on the state, as the main actor, which ensures both national defence and the deterrence of potential enemies, by military means included. Thus, the central elements of national security are power, peace and war, and the correlation between them lies in the power of the state to obtain or maintain peace through its dual capacity, either to start a war and achieve victory, or to forbid legally and/or morally weapons and war (Sava, 2005, pp. 9-10).

Complementary to the realistic vision of security, the *idealistic/liberal school* approaches security mainly from the perspective of the concept of peace, arguing the application of the principle of interdependence between states and security cooperation to achieve collective security.

The main promoter of the idealist vision was Thomas Woodrow Wilson, the 28th President of the United States of America, who was in office during the First World War. Wilsonian idealism promoted the concept of collective security and campaigned for peace based on the right of peoples for self-determination, embodied in the 14 points presented at the US Congress in January 1918. Wilson's conception led to the creation of the first international institution for collective security, the League of Nations, but the selective application of the 14 points at the 1918 Versailles Peace Conference, which marked the end of the First World War, led to the failure of idealism and created the conditions for the outbreak of the Second World War. In an attempt to explain the failure of the Wilsonian vision, Edward Hallet Carr argued in 1939 that effective collective security must be based on an international status quo accepted by all states (apud Popescu, p. 10).

The 1940s were marked by the initiation of research on behalf of the United States of America for the development of the atomic weapon, it being obtained and used during the Second World War against Japan. The atomic bomb decided the winner of this latest world conflagration and reset the international security environment. The success of the Soviet Union's development of the same type of weapon marked the second half of the 20th century, and the perpetuation of the nuclear threat was a well-known feature of the bipolar world confrontation, so popularly known as the Cold War.

The emergence of the nuclear weapon and its possession by the two major world powers reset international relations and, from a certain perspective, left the traditionalist concept of military security useless, as war could no longer be an option for ensuring world security.

A famous anecdote assumes that Albert Einstein related in a circle of acquaintances that he does not know what the Third World War look like, but in the Fourth World War, people will certainly use sticks and stones as weapons. I think that is the way the famous scientist expressed the essence of the *"nuclear age"*. Following this idea, in 1957, US President Dwight D. Eisenhower said in a speech in Washington, USA, that *"the only way to win the next world war is to prevent it"*. And he was right.

In this new *"nuclear"* context of international security, the realistic security school has *"benefited"* from growing criticism, mainly from the perspective of focusing exclusively on military power and threats, especially in the context of the end of the Cold War and the implosion of the Soviet Union, without parties having used military force against any external aggressor. If the clay colossus did not fall apart due to military aggression, then what generated the great geopolitical joy of the 20th century?

Although state relations in the international political arena are still governed by the avoidance of anarchy and fear of war, since the 1980s, security studies have begun to develop their object of analysis and consider other areas of security besides the states' military power.

Since 1991, the European Security School in Copenhagen has conceptualised social security, by extending security benchmarks, Barry Buzan and Ole Waever being the main promoters of this concept.

The evolution of the *societal security* concept started from the division of security into five essential sectors: military, political, economic, societal and environmental (Buzan, 1991, p. 19), in which the state is the reference actor for military, political security, economic and environmental, while society is the key player for social security. Thus, security acquires a double connotation, of the state and of society, the former being responsible for maintaining sovereignty, while the latter being responsible for maintaining its own identity. The survival of the two entities, the state and society, is different and distinct (Waever, 1993, pp. 23-67).

The theory of societal security distinguishes between the state and society, including from the perspective of the security-insecurity binomial, in the sense that it is not mandatory for the two to enhance each other. The society's security can generate an insecurity of the state and vice versa, especially in the case of multicultural states, with a policy of identity homogenisation of the society, as for example it happened in the ex-Soviet space. Even though the USSR was a world military power, the economic and societal realms led to its well-deserved collapse.

In fact, state borders are fixed, while society is not strictly linked to space and borders, and from this perspective, societal security refers to the identity of individuals and the way they identify as members of a community (Buzan, 1998, pp. 119-121). Thus, the existence of society is given by the very defence of its own identity, from a national, ethnic and political point of view, the national identity being characterised by affiliation to a territory, attachment to ancestors and identification as an actor in the international community.

Threats to societal security are different from those to national security and are classified into 3 main categories: migration, horizontal competition and vertical competition. Migration becomes a threat to society when it causes massive changes in the ethnic/identity composition of society, horizontal competition becomes a threat when the cultural influence of other, possibly hostile, societies becomes predominant, and vertical competition becomes a threat to integration processes or disintegration in/from supranational organisations that include a broader cultural identity.

In addition, other types of threats to societal security reside in other component areas of security, namely the military, political, economic or environmental ones, being expressed in terms of ethnic cleansing, extremism and nationalism, economic isolation, regionalisation or damage to natural resources.

As for the mechanisms for defending societal security against the mentioned threats to identity, they must be focused on strengthening societal identity through the use of cultural means that enhance social cohesion and the distinctive and specific nature of society (Buzan, Wæver, Wilde, 1998, p. 191).

Another register of threats to societal security is given by the contemporary postmodern context, where respect for human rights and acceptance of minority diversity are norms of international law, and non-compliance with these values results in various discriminations based on national and ethnic identity, religion, sex or special needs, which can degenerate even into violent actions that affect society or the state itself (Chifu, Nantoi, Sushko, 2008, pp. 165-184). Such discrimination can also be positive, by granting privileges to certain minority groups that directly or indirectly discriminate against the majority population of a state and thus alter societal cohesion. In addition, human rights abuses or inconsistencies in the application of state obligations in this area are another form of societal threat, and the best solution to combat them, along with combating discrimination of any kind, is to apply the international legal framework in the field of human rights, which is a guarantee for the survival of minorities, reducing segregation and separatism and, ultimately, increasing social cohesion.

In the analysis of the fields of security in general and of societal security in particular, the Copenhagen thinking operates with two essential terms, namely *politicisation and securitisation*. A societal issue may or may not be taken into account at the state political level, with or without public or political debates or discussions regarding the issue in question, intentionally or unintentionally.

In normal situations, of public interest for society, the politicisation of a societal problem involves drawing public attention to the problem and initiating debates and discussions, which ultimately lead to executive policy measures to resolve the situation, through concrete government measures and the allocation of financial or other resources. But what happens with societal issues that are considered to be urgent threats? In this situation, politicisation reaches an extreme variant, namely the *securitisation of a societal problem*, when the problem is presented as an existential threat to society that requires urgent measures and actions, out of the normal framework of political action.

Buzan (2008, pp. 23-25) points out that the securitisation of a societal problem occurs not only in the case of real existential threats, but also in the case of problems presented publicly by stakeholders as real threats, in which case, the manipulation of the masses is used as a mechanism by which security becomes a process of self-reference.

Thus, securitisation is an action of public discourse, through which members of a community begin to relate to a problem in terms of external threat, begin to attribute an extrinsic value to it, develop negative affect on the problem and, last but not least, calls for action to respond to and counter the threat, no matter how extreme.

Securitising societal problems generates security dilemmas, and to avoid them, the Copenhagen School also introduces the concept of *de-securitising societal problems*. De-securitisation proposes common sense solutions, such as avoiding the discussion of security issues and avoiding extreme government measures, in order to avoid escalation and violent degenerations of societal problems, returning them to political normalcy. In fact, de-security means measures to increase mutual trust within society and between identities.

Almost simultaneously with the approach of the school of societal security, at international level debates have been initiated debates on *human security*, which challenges the field of security by permuting the focus of the object of study from the state to the individual. According to this approach, the individual is the object of security, and the state is only the means of obtaining security (Karr, 2010, pp. 121–135).

An important perspective relevant to the issue of human security was presented in 1994 by the United Nations Development Programme (UNDP) in the *Human Development Report*. From the UNDP perspective, human security is based on two essential components: *security*, in the face of chronic threats such as famine, disease and repression; and *protection* against daily threats, whether they occur in the community, at work or at home. Based on these two components, human security is divided into 7 sub-components: political, individual, community, access to food, health, environmental and economic security.

Although the perspective of human security is quite permissive and comprehensive, it covers a wide range of contemporary security threats. The beginning of the 21st century finds humanity facing a diverse range of threats, especially unconventional, arising from intra-state conflicts, the spread of disease, poverty or environmental pollution, and in this context, human security theory does not negate the role of the state in ensuring security, but it points out that states themselves can become threats to the security of individuals, especially when they do not respect human rights.

Paradoxically, the very defence of human security can affect international security, edifying being the US military invasion of Iraq or the occupation of Crimea by the Russian Federation. A restrictive interpretation of the concept of human security can conclude a responsibility of large states to conduct humanitarian interventions in smaller and less developed states, with the noble goal of defending human dignity, and in fact defending human security to be only the interface for carrying out a traditional military intervention.

THE IMPLICATIONS OF INFORMATION TECHNOLOGY ON SOCIAL SECURITY

Similar to nuclear weapon which transformed the 20th century into a *"nuclear"* one, information technology has transformed the 21st century into a *"digital"* one, by increasing the merge of the physical world with the virtual one, through digitalisation, globalisation and state borders' permeability.

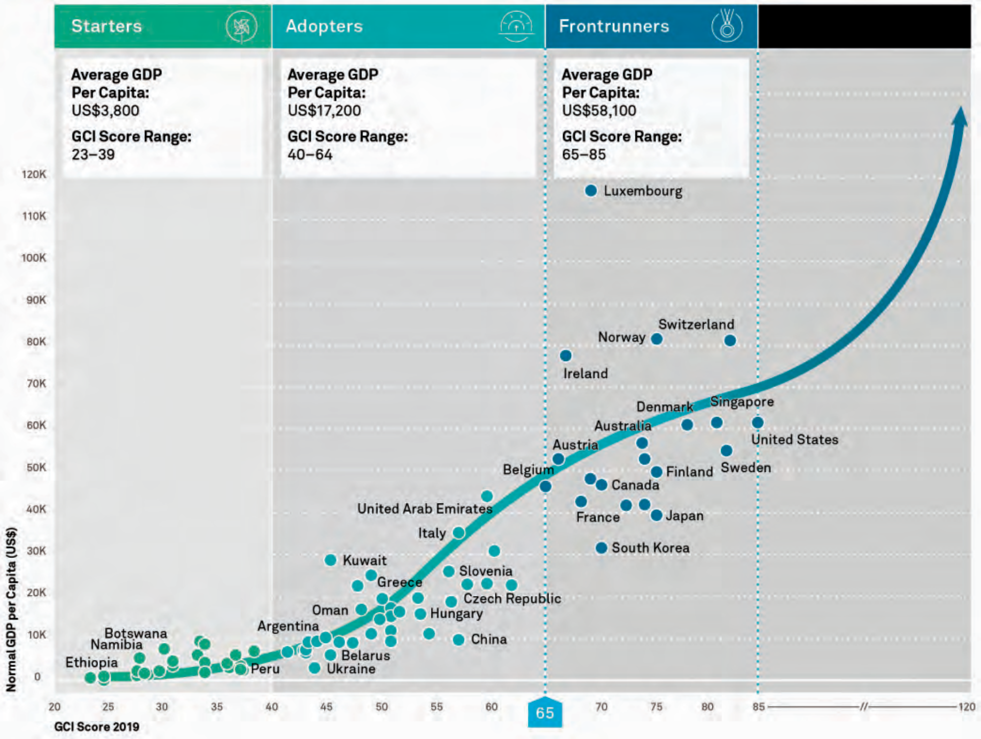


Figure no. 2: Global Connectivity Index, 2019[1]

From this perspective, the explosion of information technology development that has been taking place since the beginning of the 21st century has increasingly dominant repercussions on security in all its components. Precisely because military superiority can no longer be considered a sine qua non in winning a major conflict in the 21st century, not even in a traditional direct confrontation of the great nuclear powers, the development of information technology is slowly and surely becoming the new *"nuclear weapon"* of 3rd millennium due to its disruptive capacity, even without directly affecting human lives.

In particular, the digitisation of information, namely the advent of computers, the Internet, online digital communications, automation and artificial intelligence has generated and continues to generate substantial changes in security, starting with the diversification of actors involved in the security process. The state no longer has an exclusive role in international relations, and international and non-governmental organisations, multinational corporations, terrorist or organised crime organisations and even the individual himself are playing increasingly important roles in the security scene.

[1] Source: https://huawei.com/minisite/gci/en/.

Digitisation has increasingly important implications for security, from both the perspective of societal development and the opportunities offered to streamline and increase human productivity, from the perspective of the increasingly destructive threats it generates, and from the perspective of the influences on identity and social relations.

From the perspective of *military security*, NATO Science&Technology Organisation (2020, pp. Vi-vii) predicts that in the next 20 years information technologies will have a significant impact on the security environment, especially through the emergence of new military threats and the increase in the capabilities of destruction of smart weapons.

Military information technology will be based on four main features: *intelligence* – capabilities of integrated physical and virtual exploitation through artificial intelligence (AI) for conducting security analyses based on focused knowledge of targets; *interconnectivity* – technologies of symbiosis and integrated exploitation of physical and virtual domains, based on networks of sensors, organisations, individuals and other autonomous agents connected by new coding and distribution methods; *distributivity* – ability to collect, store and analyse information on a global scale and enhance new disruptive military effects; and *digitisation* – the digital fusion of human, physical and information domains to increase the disruptive effect of the military.

Regarding the new capabilities of *military information technologies*, designated by NATO as *emerging and disruptive technologies*, these are: *digital data-AI-autonomy* – the synergistic combination of autonomy, big data and AI through multiple sensors within autonomous entities, physical or virtual, which will increase the strategic military potential and benefit the operational decision; *digital data-AI-biotechnology* – the combination of AI with big data will contribute to changing human behaviours, by creating new drugs, genetic changes, manipulation of chemical reactions and new sensors; *digital data-IA-materials* – the combination of IA with big data will contribute to the creation of new materials with unique physical properties that will be used primarily in the military field; *digital-quantum data* – quantum technologies will increase C4ISR's capabilities for collecting, processing and exploiting data and information; *space-quantum space* – the ISR military architecture will be based on new quantum sensors positioned in space; *outer space-hypersonic speed-materials* – military systems will be easily adaptable to specific and particular missions, will be produced at low cost, miniaturised, from exotic materials, will have the ability to store energy and will be able to explore outer space at supersonic speeds. Basically, through the new military information technologies, the popular TV series Star Trek has great chances to become a reality.

From the perspective of *political and economic security*, the disruptive effects of information technology have already begun to be visible since 2016, in the public scandals regarding the Brexit campaign, Cambridge Analytica, or the influence of the US presidential campaign.

Digitisation has changed the international labour market, and not all people have been able to adapt to the new economic conditions, with unemployment rates rising for the population without digital skills. At the same time, digitalisation has stimulated globalisation, the world's population being increasingly interconnected, with direct effects on the world economy. It is estimated that an annual increase of 10% in economic digitisation generates an annual increase in gross domestic product per capita of 0.5-0.62%, and in 2010 the annual growth in actual terms generated by digitisation was $ 395 billion (El -Darwiche, Singh, Ganediwalla, 2012).

And what are the effects? Are they just economic? It seems that not and, more and more obviously, globalisation through digitalisation, translated by internet connection, blockchain, algorithmization and robotisation, forms a new form of political risk, at least in Euro-Atlantic democracies, based on changing electoral behaviours, the eloquent example being the vote in Great Britain for the referendum organised for leaving the EU.

In an attempt to study political risk, research indicates that an increasing number of the electorate is not in favour of globalisation and fails professionally to keep pace with the exponential growth generated by digitalisation. Given the automation of the production of goods and services, the loss of low-skilled jobs turns into a *political risk*, and innovation affects people's confidence in information technology and vice versa. People affected by a lack of trust begin to believe that information development is based on greed and is increasingly demanding that the situation should be regulated by stricter laws (Hoogeveen, 2017).

Like a vicious circle, digitalisation generates fear of job losses in the low-skilled population, and the political environment does not have an adequate set of measures to respond to this situation, promoting even more globalisation, free trade and international competition. Instead, the economic environment prefers to favour information technology, investing much more consistently in equipment than in its own employees. The political risk is self-enhancing in populism and extremism.

At the same time, information platforms that provide economic services are increasingly accused of carrying out actions of national tax avoidance, and the issue is being intensely discussed at EU level (Policy Department A: Economic and Scientific Policy, European Parliament, 2018). For example, in the period 2013-2015, it is estimated that Alphabet Inc (Google) and Facebook avoided EU-wide taxes of 5.1-5.4 billion euros (Tang, Bussink, 2017).

From the perspective of *societal security*, specialised studies are already beginning to clarify a number of implications and types of social threats that digitalisation generates. Thus, recent studies indicate that information technology can generate threats and dangers within six social values: personal data protection, autonomy, digital data security, human dignity, justice and the balance of power (Royakkers et al., 2018).

If we were to paraphrase a famous Romanian writer, we would say that, with digitalisation, the protection of personal data is so sublime that it is almost completely missing. If smart phones no longer claim to fully protect our privacy, the digitalisation of homes, by integrating and interconnecting smart equipment in personal cars, TVs, refrigerators and even the toothbrush, shatters our privacy and make our personal data available to multinational companies that produce the goods in question.

According to the European Commission, *"over 90% of Europeans say they want the same data protection rights everywhere in the EU and no matter where the data is processed"* (Communication from the Commission to the European Parliament and the Council, 2020), and this very main argument was the basis for the adoption of the General Regulation on data protection (RGPD) (EU) 2016/679 on the *protection of individuals with regard to the processing of personal data and the free movement of such data*, which has become mandatory since May 2018. Only the passage of time will prove to EU citizens the extent to which this regulation has effectively protected their personal data.

In terms of the autonomy of technology, the security challenges lie in the limits it acquires in terms of paternalism, control, influence and behavioural manipulation. If most of us agree that, for example, in the case of cars, distance sensors or automated speed limiters are useful in preventing accidents, what happens if technology involuntarily controls us or manipulates us behaviourally by deciphering our conscious or unconscious preferences and choices?

Digital addiction and behavioural manipulation through digitised platforms have generated psychological studies that take the form of a new field, cyber psychology, and current debates focus on digital dementia, memory impairment and impairment of cognitive abilities by excessive use of information technology (Born, 2014).

Virtual data security has been a constant challenge in recent years. Practically, recent experiences show that any device that incorporates information technology can be accessed and controlled unauthorised, and hacking is not used exclusively for personal devices, but also for organisational devices, whether state or public or private. Precisely due to the special amount and sensitivity of digital information, cybersecurity is an already developed and extremely important field, and threats such as virtual identity theft, cyberattacks or cyberterrorism are already part of everyday life.

More and more recent studies conclude that the development of robots, biometric systems, automated decision-making systems or social reality systems begin to affect human dignity more and more deeply, with serious psychological effects, such as dehumanisation, standardisation, ignorance of morality, and, last but not least, alienation. The increasing robotisation in the economic field, health or even the military, affects the establishment of human interpersonal connections, and the decision-making process is dehumanised. Biometric systems are not 100% efficient, but are credited with 100% confidence. Their mistakes create direct human consequences and, paradoxically, all those affected must prove their *"innocence"*.

In addition, digital systems are programmed to make decisions based on efficiency and not morality, and virtual reality systems or virtual social networks create dependence and replace direct human relationships, the *"social animal"* being transformed into a *"virtual lonely"*.

In terms of social justice, information technology can create injustice precisely by the lack of accuracy in 100% of cases, as it is the case with biometric facial, voice or fingerprint recognition systems. In addition, the change in the labour market through the emergence of platforms that provide services through people who have the status of collaborators and not permanent employees creates the premises for ignoring their rights derived from labour law, economic exploitation, discrimination and even social exclusion.

Last but not least, in terms of the balance of power between information technology and social consumers, at least for the time being, it is in favour of the former. If the products offered are controlled by software by the manufacturers, they can decide at any time how long they will be used, and users are inadvertently rendered unable to use the products. Most acutely, the situation is felt in the case of smartphones that are designed to be replaced as often as possible.

In addition, the competition between digitised and real companies is uneven, eloquent being the cases of hotel service platforms or ridesharing services, which do not fully comply with the same rules and restrictions as traditional hotels or taxi companies. In this regard, specialists refer to the term digital feudalism, understanding by this that people have more and more the role of *"digital slaves"* enslaved to the *"digital nobility"*.

At the same time, the state begins to play an increasingly important role in collecting data from digital citizens, eloquently being the example of the Chinese government, which has established a system of social credit assigned to citizens, relevant to important areas such as access to education, employment or access to funding.

In terms of environmental security, studies show the increased impact of digitalisation on the environment, in particular through the carbon emissions generated by the production of electricity needed for the operation of the digital industry. A precise impact of digitalisation on the environment cannot yet be estimated precisely because of the diversity of entities involved, from digital companies, internet companies, data servers, data transmission antennas, information technology equipment, creators and consumers of digital content.

Thus, in 2015, it was estimated that only data centres generate 2% of global carbon emissions, and the Internet consumes 8% of the energy produced by the United Kingdom (Hodgson, 2015). For comparison, studies in 2019 estimate that digital technologies emit double, 4% of global greenhouse gas emissions, forecasting an increase of up to 8% by 2025, with total energy consumption estimated at 45% by digital production and 55% by digital consumers (Efoui-Hess, 2019).

CONCLUSIONS

Security is multidimensional, and this multidimensionality is manifested simultaneously in terms of the form of reporting objective and subjective threats and dangers, and in terms of security content and component areas.

Throughout the article we have highlighted how information technology has profound effects on society and security, in all its component areas, military, political, economic, societal and environmental, the field of information technology being confused as a separate area of security.

The automated collection and analysis of digital data has very real effects on people's lives, and offline and online environment is merging more and more deeply. Automation based on the automatic collection of digital data, big data and artificial intelligence algorithms is gaining more and more influence in the field of social decision control, to the detriment of people, and has increasingly persistent manipulative effects through behavioural influence mechanisms known as social engineering. At this point, it is a reality that the analysis of behaviour performed through digital activity reveals the main personality traits and political, religious or sexual preferences. Is there more needed?

The rapid advancement of digitalisation affects the essence of social security, its identity. From the inequality of the digital power balance, the automation of military capabilities, the loss of jobs in the production of goods and services, the avoidance of taxation of digital products, the automation of economic and social decisions, discrimination, social injustice, behavioural manipulation, diminished control over personal data and privacy, inequality, dehumanisation, alienation, declining quality of life, loss of human cohesion and inclusion, unsustainable development and environmental damage etc., all of which affect perceptions of security and further subjectivize the reality of security, with serious effects on societal security as a whole.

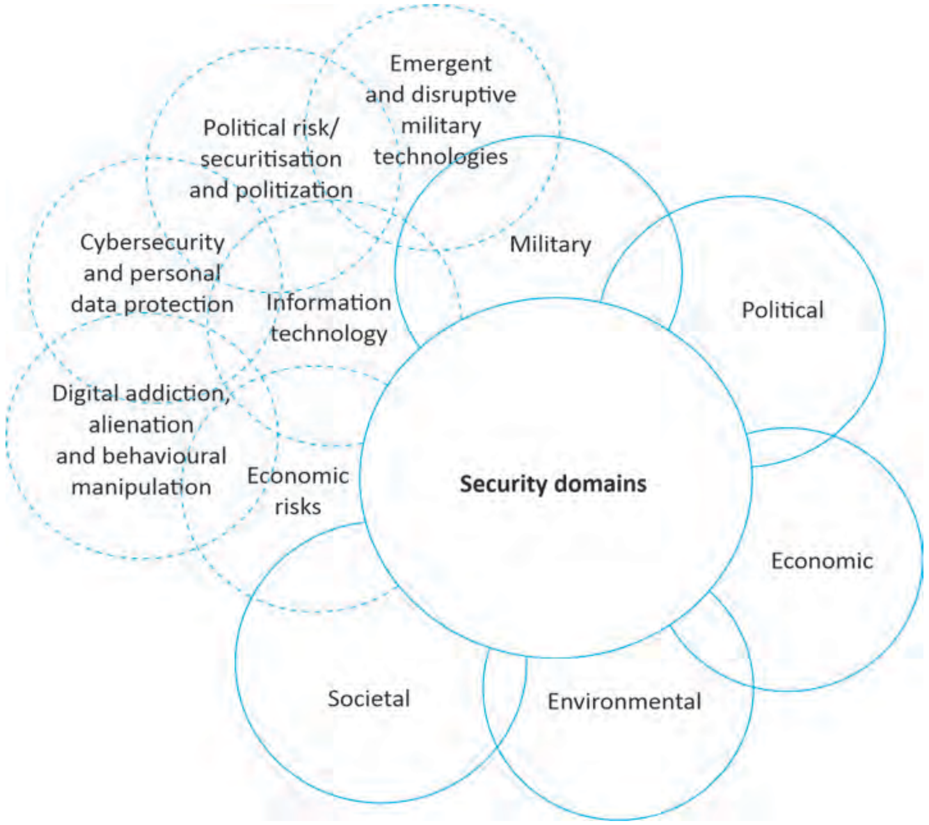

Emergent and disruptive military technologies
Political risk/ securitisation and politization
Cybersecurity and personal data protection
Information technology
Military
Political
Digital addiction, alienation and behavioural manipulation
Economic risks
Security domains
Economic
Societal
Environmental

Figure no. 3: Domains of contemporary security

Digitisation causes political, economic and societal effects that affect the very way of establishing national and international social relations, both objectively, through the challenges of ensuring digital security and subjectively, by distorting perceptions, reasoning and manipulation of security behaviours, individual and group, national and international.

So far, the greatest fear of states has arisen from the threat of military anarchy. Nowadays, states and society should look deeper into whether or not moving towards digital anarchy. Digital technologies have already profoundly transformed organisations, whether public, private or state, and the negative effects, threats and risks involved must be addressed in a comprehensive and multidisciplinary manner, in order to reduce and eliminate digital anarchy in all areas of security, military, political, economic, societal and environmental.

Unfortunately, the time left to counteract the negative effects is not unlimited, because, unlike the industrial revolution that marked the 20th century, the digital revolution has a much higher speed of propagation and transformation, which is increasing from year to year. Digital regulation is still in its infancy, and the total lack of regulation is materialised in the lack of defence of the state and society against digital threats with serious repercussions on societal security.

Debates about the benefits, threats, risks and challenges posed by the development of information technology are far from exhausted. If effective collective security is to be based on an international status quo accepted by all states, therefore we believe that the actors involved, from the individual, public and private organisations and states, should be encouraged to work together both nationally and internationally for better knowledge and regulation of the digital domain in order to reduce and eliminate the full spectrum of digital threats, and the scientific community has a moral obligation to research and support these efforts.

BIBLIOGRAPHY:

1. Born, S. (2014), *Do digital media lead to 'digital dementia'?*, Alumniportal Deutschland, https://www.alumniportal-deutschland.org/en/science-research/news-from-science/digital-dementia-michael-madeja-brain-research-manfredspitzer/, retrieved on 15 September 2020.
2. Bușe, C., Hlihor, C. (2004). *Security Paradigm Between Classic and Modern.* In Euro-Atlantic Studies, no. 7, București: Editura Universității București.
3. Buzan, B. (1991). *People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era*. Essex: Longman.
4. Buzan, B., Wæver O., Wilde, J. (1998). *Security: A New Framework for Analysis*. Londra: Editura Pinter Publishers.
5. Chifu, I., Nantoi, O., Sushko, O. (2008). *Securitate societală în regiunea trilateralei România-Ucraina-Republica Moldova*. București: Editura Curtea Veche.
6. Deutsch, K.W. (2006). *Analiza relațiilor internaționale*. Chișinău: Editura Tehnică.
7. El-Darwiche, B., Singh, M., Ganediwalla, S. (2012). *Digitization and Prosperity*. In Strategy+Business, no. 68, https://www.strategy-business.com/issue68-autumn 2012, retrieved on 15 September 2020.
8. Efoui-Hess, M., (2019). *Climate crisis: the unsustainable use of online video. The practical case for digital sobriety*. The Shift Project, https://theshiftproject.org/wp-content/uploads/2019/07/2019-02.pdf, retrieved on 15 September 2020.
9. Hlihor, C. (2008). *Politici de securitate în mediul internațional contemporan*. Iași: Editura Institutului European.
10. Hodgson, C. (2015). *Can the digital revolution be environmentally sustainable?*. The Guardian, https://www.theguardian.com/global/blog/2015/nov/13/digital-revolution-environmental-sustainable, retrieved on 15 September 2020.

11. Hoogeveen, M. MSc. (2017). *Impact of digitalization and globalization on political risk*. In Compact, no. 2, https://www.compact.nl/en/articles/the-impact-of-digitalization-and-globalization-on-political-risk/, retrieved on 15 September 2020.
12. Kerr, P. (2010). *Human Security*, apud. Collins, A., Contemporary Security Studies. New York: Oxford University Press.
13. Kissinger, H. (2002). *Are Nevoie America de o Politică Externă?*. București: Editura Antet.
14. NATO Science&Technology Organization (2020). Science&Technology Trends 2020-2040, Brussels.
15. Policy Department: Economic and Scientific Policy. European Parliament (2016). Tax challenges in the digital economy, https://www.europarl.europa.eu/RegData/etudes/STUD/2016/579002/IPOL_STU(2016)579002_EN.pdf, retrieved on 15 September 2020.
16. Popescu, C. (2008). *Concepte strategice specifice mediului de securitate contemporan*. București: Editura Universității Naționale de Apărare *"Carol I"*.
17. Royakkers, L., Timmer, J., Kool, L., van Est, R. (2018). *Societal and ethical issues of digitization*. In Ethics and Information Technology. no. 20, https://doi.org/10.1007/s10676-018-9452-x, retrieved on 15 September 2020.
18. Sava, I.C. (2005). *Studii de securitate*. București: Editura Centrului Român de Studii Regionale.
19. Tang, P., Bussink, H., (2017). EU Tax Revenue Loss from Google and Facebook, https://www.paultang.nl/wp-content/uploads/2018/03/EU-Tax-Revenue-Loss-from-Google-and-Facebook.pdf, retrieved on 15 September 2020.
20. United Nations Development Programme (1994). Human Development Report. New York: Oxford University Press.
21. Waever, O., Buzan, B., Kelstrup, M., Lemaitre, P (1993). *Identity, Migration and the New Security Agenda in Europe.* London: Pinter Publishers.
22. Communication from the Commission to the European Parliament and the Council (2020), https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_ro#relatedlinks, retrieved on 17 September 2020.

INFORMATION WARFARE, SECURITY INTELLIGENCE AND MILITARY INTELLIGENCE.
– A SHORT THEORETICAL APPROACH –

Teodor BADIU

National Intelligence Academy, Bucharest

In research, discussions from public space and materials designed and disseminated by media trusts, the issue of hybrid warfare/hybrid threats is often analysed either as a phenomenon or as a specific factor of an event. However, due to the complexity of the subject, confusion is often made or the concepts are mixed as the subject becomes even more ambiguous. In addition, the excessive use of simple terms such as "information manipulation", "propaganda", "misinformation", "influence", in the public space, has led to an alteration of their meaning and an ambiguity of the effects that these terms have on the perception of threat. On the other hand, in this context, the role and relevance of security and military intelligence in the management and limitation of hybrid warfare/hybrid threats has been little discussed. Thus, this paper tries to detail in a succinct manner (due to the complexity of the topics), at a theoretical level, the concepts of security intelligence, military intelligence and information warfare.

Keywords: information warfare; security; deception; multinational exercises; asymmetrical confrontations;

INTRODUCTION

Starting from the Ukrainian experience and the situations of information interference in the internal affairs of other states, *hybrid warfare/hybrid threats* represent the factor of instability and insecurity that acts according to the specifics of the operations, regardless of the nature of the actors. Hybrid warfare has enveloped the international security environment, especially in the European space, because of the actions of the Russian Federation, starting from 2014, which reminded the EU and NATO that the Russian Federation was willing to use all means to achieve its strategic objectives, including regaining its sphere of influence over the Eastern European states.

In this regard, we can consider *hybrid warfare* as the factor that establishes the context of information warfare and reduces the distance between security intelligence – its role is to secure the elements that operate the national system such as society, economy, political environment, infrastructure etc. and military intelligence – whose function is to gather information about the armed forces of the opponent or a possible one, disseminating the information obtained to a *military decision maker* who can formulate strategies or organise/reorganise the military forces as needed. Traditionally, their activity gets intensified when there is a declared state of conflict between at least two actors, but, at present, *hybrid warfare* exists without states declaring their actions and without any declared conflict. A major problem of *hybrid warfare* is that it makes the origins and forms of threats ambiguous, which has led to the necessity of increasing activities such as monitoring, preventing or repelling by institutions specialised in military and security intelligence. In addition, in the issue of information warfare, the context of *hybrid warfare* has produced some changes: information warfare has traditionally been a component of armed conflicts between actors (such as asymmetric or irregular confrontations, unconventional approaches, active measures etc.); its scope has extended to the civil one, without requiring the official declaration of the beginning of hostilities.

Next, we will approach, from a theoretical point of view, the relevance of information warfare, security intelligence and military intelligence to understand some of their peculiarities.

DEFINING INFORMATION WARFARE, SECURITY INTELLIGENCE AND MILITARY INTELLIGENCE

Hybrid warfare is an operational concept that integrates a wide range of elements, and in this sense, it is predictable that it affects domains from the economic, political and military to the social and cultural ones. However, events of recent years since 2014 – the annexation of the Crimean Peninsula and the emergence of separatist forces in eastern Ukraine, the political rise of extremist groups in Europe, foreign involvement in elections and referendums, the proliferation of conventional arms between NATO and the Russian Federation, the wargames[1] initiated during the multinational exercises, the disinformation and de-legitimisation campaigns initiated by the Russian Federation, the attempted assassination of the defector Sergei Skripal, the need to rethink CBRN protection measures (context of the international spread of COVID-19 virus) – demonstrate the need to include security intelligence and military intelligence in a common and inclusive approach. Overall, these events can be understood as segments that make up hybrid warfare. Until recently, the role and objectives of security intelligence and military intelligence were seen as something limited. Nowadays, the mutations of threats have led to an amalgam of information and military actions whose effects have been felt especially in Eastern Europe.

In this equation, *information warfare* has an essential role in the degradation of security environment. This is a term associated with hybrid warfare (but not only, being connected with asymmetric, irregular and unconventional warfare, active measures, public diplomacy etc.) (Theohary, 2018, pp. 4-5), which has dual valence, offensive and defensive, and which has distinct forms of manifestation depending on the state of war or peace. NATO defines the concept in strictly military terms, from the perspective of cyberwar where information warfare consists of *"undertaking actions to obtain computer field superiority through deterioration of enemy information technology systems and protect own devices"*. (AAP-6, 2018, p. 430). However, as we talked about the context, we notice that the information warfare is not only manifested in the military sphere, but it can also extend to the social and political area or can be interdisciplinary.

The broad spectrum in which information warfare can operate makes it a much more effective weapon, due to the fact that (Molander et al., 1996, pp. 15-29):

- the cost-benefit ratio can be maximised due to relatively low costs. Unlike the maintenance and deployment of an army whose existence poses a threat or leads to a security dilemma, the infusion of an information environment with rumours, partially true or ambiguous information, can lead to misperceptions and an escalation of fear. Also, the support and organisation of the information warfare can be provided by a small number of individuals, being quite accessible;
- the blurring of traditional borders due to economic, social, political and military interdependencies has led to an alteration of the individuality of state actors. The connection of states and private actors to the global information system (via the Internet, for example) has amplified the difficulty of distinguishing between external and internal threats in the context of information warfare;
- their perceptions and management can be problematic in the sense that the flow of information abounds with official, unofficial, sequential, conspiratorial, erroneous, false, ambiguous information etc., making the society vulnerable to alterations of reality or information intoxications. Manipulation of information through techniques and technologies can allow a wide range of actors to undermine the authority and even the legitimacy of institutions, states or international organisations;
- the difficulty of early warning and rapid impact assessment determines a major vulnerability to surprise information attacks, the actors being limited as a possibility of prevention or response. Doubled by the difficulty of seeing, in the shortest time, which was the target, the evaluation of the effects may require additional time and costs;
- the interoperability between allies or members of an international organisation leads to the synchronisation of C4I systems to ensure coherence, but even if their own systems are well secured, the weakness of an allied system can lead to the penetration of the overall system.

With regard to information warfare, it should be noted that its pillar consists of *information operations* (IO), which can be defined as the integrated employment of information capabilities in accordance with other lines of operations to influence, interrupt, corrupt or usurp the decision-makers of opponents while own systems are protected (*Dictionary of Military and Associated Terms*, 2020, p. 104). In principle, IOs serve the purpose of making the opponent/target behave, or not, in a certain direction by using segmented information (extracting information from a specific context), propaganda and intentional (determined by a deliberate and organised action) or unintentional misinformation (caused

[1] Wargames are an analytical form that simulates tactical, operational and strategic aspects of a conventional confrontation. They are usually used to examine the concepts of combat, to train analysts and commanders, to develop scenarios and to evaluate the effects of subsequent or ongoing ones.

by erroneous actions, misunderstanding or involuntary degeneration of information). The following types of operations are subcategories of IOs (Theohary, Ibid., p. 3):

- Psychological operations (PSYOPS) – involve the type of operations initiated, in order to influence and exploit the emotions, motivations, perception and behaviour of the target at the cultural and cognitive level;
- Security operations (OPSEC) – represent actions and measures taken for defensive purposes, which identify and analyse essential information, disruptors of an ongoing operation and the protection of all elements that contribute to the operation. For offensive purposes, it means gathering information to facilitate the understanding of the opponent, being also the process of slowing down the possibility of making a decision in a timely manner by the opponent's decision-makers;
- Electronic warfare (EW) – is defined as the accumulation of military technical actions, carried out using electromagnetic waves and signals to support ongoing operations, protect their own equipment and attack the computer systems of opponents. As more well-known activities, we can mention the jamming of communication systems, encryption and decryption of channels, the use of satellite positioning systems (GPS) etc.;
- Cyber operations – are the actions carried out in cyberspace that can range from system interruption and viruses to support for integrated systems and protection of own systems;
- Deception – can involve all or a large part of the types of operations presented in order to misleading the opponent. By *"accidentally"* sending false reports and documents to foreign agents, falsifying radio channels that are intercepted, organising misleading displays etc. (Herman, 1996, p. 170), and depending on the information that the opponent has, could be exploited opportunities that, in the end, lead to confusion at the decision-making level.

Considering the typologies of operations, we notice that information operations could have a coercive character that can be translated by influencing the adversary's decision-makers or the civil environment in guided directions through covered operations. Hence, if we talk about the soft approach, information operations can contribute by creating a positive image in relation to other actors to determine legitimacy or long-term advantages, or just to support public diplomacy.

Though IOs are generally initiated and planned by specialists from the military field or intelligence services, their applicability extends also to the civilian area. So that, in recent years, discussions about *information disorder* (Wardle et al., 2017, p. 20) – a concept much broader encompassing fake news, false news, misinformation and grey propaganda – spreading in the media, mainly in key

moments such as elections, referendums, major protests, crisis situations etc. have intensified because of their effects that affect relations between authorities and their own citizens or between different social groups. We can say that the spectrum of information disorder can contribute to the process of deception because it delivers to a target certain information that is partially true or false. It means that it must create a specific perception or make the target act in a particular direction. Seen from a psychological perspective, the essence of information disorder lies in the subjectivism of the target, where it is not important how the story is presented, but the story as such, which can favour a given context.

To exemplify, we can address the issue of social media platforms as Facebook and Twitter, which are increasingly confronted with information disorder that uses their infrastructure. As a result, since 2016 they have tried to initiate some more austere regulatory actions and measures like stopping the spread of fake information through posting and distribution of content, and elimination of accounts that are dubious and disseminate erroneous and contradictory information (Polyakova, Fried, 2019, p. 12). On the other hand, other companies such as Google and YouTube have shown little transparency regarding the measures taken. More exactly, Google has allowed known disruptors such as Sputnik or RussiaToday to remain in the top of search engines, while YouTube has changed only the terms and conditions for extremist and insulting videos without supporting a solid campaign to remove them (Ibid., pp. 13-14). In this regard, the 2019 attack from Christchurch in New Zealand, when a radicalised individual broadcast the attack on two mosques on the internet can be approached as an example of the platforms' inability to stop the spread of toxic information. Only after this incident YouTube did remove from its platform the video Remove Kebab, considered to be an anti-Muslim propaganda song from the Yugoslav wars. It is worth mentioning that the killer on the way to the two mosques listened to this song in his car.

Social media tries to block, in different proportions, the tools and effects of *information operations*, but they will not be able to cope because of the distinct specificity. IOs have a military origin, based on a military doctrine where civilian and military personnel conduct planning and execution. Due to this fact, private companies in the social media sphere are at a disadvantage because their response is from a strictly technical perspective, and from a cultural point of view, they are related to the principles of economic markets. Organising an adequate and efficient response would involve the establishment of a specialised department composed of staff trained in intelligence domain that would probably not be legal and sustainable in terms of costs and benefits.

Thus, we note that with regard to IOs and implicitly the information warfare, states are the ones that must react because they are the only ones with qualified personnel in execution and combat, moral and legal legitimacy, consistent material resources, complex bureaucratic apparatus and specialised institutions. In this respect, the state may have a monopoly and in the context of international competition, the need for security could enhance the significance and activity of security and military intelligence.

After World War II, Sherman Kent introduced in the specialised literature the notion of *security intelligence* as a distinct form by the military intelligence. He defines it in two directions: as the intelligence work behind the police activities that deals with the protection of the state and citizens; and as an activity designed to identify those internal disruptors such as clandestine agents, traitors, elements of organised crime and violations of the (federal) law (Kent, 1965, pp. 209-210). This perspective on security intelligence tends to be closer to police work, but if we compare the institutions of several countries that deal with security intelligence we will see that they have developed a specificity related to culture, the past and tradition of the institution, the regime they belong to, the importance of the institution in relation to other institutions, the financial resources available, the degree of qualification and the number of staff etc. In general, the interest subjects of security intelligence consist in counterterrorism, combating subversive operations carried out on the national territory, counterintelligence and combating organised crime activities. Security intelligence, in theory, excludes activities in the political, economic, tactical and military fields, and is considered different from *information security*, interspersed only with counterintelligence – security intelligence and information security would aim jointly at preventing/combating information leaks and protecting information systems (Robinson, 2010, pp. 113, 207). Moreover, although in theory institutions accredited in the area of security intelligence should deal only in the area of internal protection, in practice, there are particularities of institutions in various states that lead to notable differences.

Taking as an example MI5 (Security Service) from the UK, FBI from the USA and FSB from the Russian Federation, we can notice distinct approaches to national security, each including activities that go beyond the area of internal security or focusing on specific areas. We can exemplify the situation of the FSB, which, after its merge with FAPSI – Federal Agency of Government Communications and Information – began to extend its attributions from internal security to a mix of defence and offense by undertaking activities specific to electronic warfare. In comparison, MI5 offers an increased attention to counterterrorism and extends its area to the defence of economic welfare and the democratic parliamentary regime – as an ideological/identity component (Ibid., pp. 92, 209). Michael Herman explains security intelligence as a separate entity from decision-makers whose role

should be to provide information rather than advice. Although security intelligence has to deal with internal threats, they, however internal they may seem, have an external origin so it is vital to inform decision-makers through analysis and forecasts that also include external elements (Herman, p. 34). This adaptation is due to the transition of the security paradigm from the Cold War system, based on an ambivalent conflict between the Warsaw Pact and NATO, to a multipolar system marked by the uncertainties of the hybrid warfare. If in terms of intelligence work, the Cold War period was focused on gathering information, organising and destructuring subversive operations, espionage and counterintelligence, to understand the intentions of the opponent, now we are witnessing a paradox. It is not uncommon when external intelligence is also collected from the national territory, while security intelligence is collected from outside national borders, and the targets may consist more in subjects than in the actors themselves, especially in the context of dilution of the meaning of security intelligence as a strictly internal process (Ibid., pp. 47-49).

Regarding military intelligence, it can be said that there is a long tradition, as a result of the need for armed forces to know vital information such as capabilities, number, specialisations, morale, troop disposition, strategies, command centres etc. of opposing forces. Thus, the definition of military intelligence begins with the perspective of Carl von Clausewitz who described the collection of information in time of war as necessary, but contradictory. Either there is a situation when some of the information is false, and another part consists in uncertain information that at some point will contradict each other, or the information supports each other and in the whirlwind of a decision that seems appropriate proves to be wrong due to erroneous, false or exaggerated information (Clausewitz, 2014, p. 38). In short, military intelligence is that component of intelligence that is concerned with issues specific to the military area, the capabilities of states, foreign organisations, or ongoing multinational military operations (DoD, p. 91). We can add that the military intelligence tries to discover the weaknesses of enemy military architecture, offering the Command the chance to streamline its combat actions with minimal risks. On the other hand, it tries to analyse and discover the weak points in own and the allies' defence system. However, in light of the proliferation of conventional weapons and wargames in recent years, the topics of defence intelligence seems to remain in the spotlight of security institutions. *Defence intelligence* can be considered a subcategory of military intelligence, whose topics are also of interest to the political environment. The object of activity is focused on the supervision of external military actions and local or regional wars, this including autonomous or sustained by external aid insurrections; situations in which combined politics, violence and subversive operations lead to the use of armed forces; the failure of states as a result of inter-ethnic, religious, ideological conflicts, etc. (Herman, p. 50). Moreover, as topics of interest to defence intelligence there are also defence industries, arms exports, technological developments in military technology, the proliferation of weapons of mass destruction (tactical and ballistic) etc.

A fundamental aspect of intelligence, which cannot be neglected, whether we are talking about security or military intelligence, is deception. NATO defines it as *"those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests"* (AAP-6, p. 272). This is not a new practice, leaders and generals have used it since Antiquity in achieving their goals, but conceptually, the complex variant of deception is military deception (MILDEC). Strictly speaking of its operational nature, military deception could not be considered part of intelligence, given that it coagulates specific elements and activities such as OPSEC, PSYOPS, EW, intelligence gathering, counterintelligence etc. However, it can be considered as a defensive means in the case of security intelligence, and offensive in the case of military intelligence. Although it seems strange that it is assigned to the first category, in the context of information warfare, MILDEC can generate various forms of perception of politicians, military personnel and civilian targets, causing erroneous actions or inopportune inaction of governments, or causing civil society to put pressure on governments in a certain direction. In particular, we note that MILDEC's spectrum of soft activities is composed of influencers, information operations, covered financing operations of political groups or media trusts; and the hard spectrum consists in covert support for opposition groups, resistance, insurgency or terrorist forces, and sabotage and paramilitary operations (Herman, p. 55).

Regarding military deception, the literature is abundant and includes comprehensive details, from deception targets and objectives to the conduits, networks and filters used in deception. The subject MILDEC represents in itself a vast research topic, which combines theoretical and practical aspects in a subtle art, but for this study, we will highlight some fundamental theoretical aspects.

MILDEC's role is to create a *story of deception* that the opponent can take as such, and all the evidence related to the story look veridical. The story of deception is a narrative or a brief statement, constructed according to the perspective and specificity of the target – like mental structure, values, specific culture and its expectations – and which is strengthened by misleading events (Field Manual 3-13.4, 2019, p. I-5). Regarding the types of deception, two categories can be identified:

1) ambiguity-increasing, which aims to generate confusion and internal conflict over adverse decision-makers through a continuous flow of seemingly plausible information, drawing their attention from a set of activities to another;

2) ambiguity-decreasing, which involves the manipulation and exploitation of pre-existing thinking and beliefs of adverse decision-makers, by guiding the target to the wrong place at the wrong time, in conditions of maximum vulnerability (Ibid., pp. I-6-17). Alternative terms such as Type-A (ambiguity-increasing) deception, to amplify ambiguity, and Type-M deception (misleading deception), to reduce ambiguity, can also be found in the literature, and passive and active forms of deception can be identified. The passive form is based on the actions of covering and camouflaging one's own intentions and/or capabilities towards the opponent, while the active form consists of one's own deliberate actions, to present to the opponent the intentions or capabilities he does not possess (Shaw, 2014, p. 3). MILDEC uses a narrow range of tactics to concretely serve to different missions objectives as follows:

- *Ruse* – deliberate actions to alter reality through information;
- *Diversion* – intentional distraction of the opponent from a subject/objective of interest or from carrying out an attack;
- *Feint* – offensive actions that involve direct contact with the opponent and whose purpose is to mislead the opponent regarding the place and/or time when an attack will take place;
- *Demonstration* – show of strength initiated in order to determine the opponent to choose the most disadvantageous course of action;
- *Cover* – actions aimed at masking the preparations or initiating an offensive operation, depending on the situation associated with conditioning;
- *Display* – actions organised to support the story of deception by simulating, disguising and/or highlighting the capabilities and composition of allied forces (Ibid., p. 6).

It must be reaffirmed that at the heart of these actions is the story of deception, which is a product of the imagination. This requires organised and disciplined thinking, so that the logic of the story is not interrupted and the target can perceive it visibly – the exaggeration of its subtlety can make the target to ignore the story of deception. The deception operation must be done from the perspective of the target, and his ensemble must be a general description of the whole deception. Thus, the story of deception must be verifiable (the target can confirm it through its own channels or with the help of his allied intelligence structures), executable (the existence of the necessary authority and resources), credible (diminishing suspicions and doubts on the part of the target) and consistent (initiators of deception must know the degree of training of the target to not exaggerate or diminish the complexity of the story) (Field Manual 3-13, 4, pp. II-10-II-11). For this reason, field-specific maxims are often used in misleading processes to facilitate the organisation and execution.

Thus, we detail only a few maxims (CIA, pp. 5-20, 22-26, 32-33) that are relevant to this study:

a) *Magruder's principle* aims to capitalise the opponent's beliefs, using them in altering reality and examining the possibilities that may be to his disadvantage. This principle can be exemplified by the planning of the invasion of Normandy, where information showed that the Germans were expecting an Alliance offensive in the Pas de Calais region, being a setback of German plans to invade Britain.

b) *Limitations to human information processing* are processes of human cognition that, almost universally, in specific situations present syncope of processes. In this sense, syncopes can be exploited, which leads us to the law of small numbers and the predisposition to *conditioning*. The law of small numbers refers to the human tendency to generalise in the case of small data sets. Conditioning is the accustoming of the opponent to a certain situation or will, which was carried out over time by transmitting repetitive stimuli. Another limitation is the human tendency to omit small changes or small details.

c) *The multiple forms of surprise* consist of location, force capabilities, intention, specific style and timing. Although not all can be achieved in an operation, the emphasis must be on limiting a number of relevant elements. The use of false alarms is one of the main elements of surprise by conditioning the opponent not to respond immediately to the apparent imminent threats and by misleading as the opponent directs his attention, resources and staff where false alarms indicate.

d) *A choice among the types of deception* is necessary due to the fact that their extensive use can lead to distrust of the target in the appearances that are served to him. Thus, in this situation we opt to reduce the ambiguity, although if the target already has some real information, it may be recommended to increase the *"noises"* – increase the target's access to false alternative information and/or evidence that prove the authenticity of the false information that has been delivered.

e) *A sequencing rule* refers to the need for misleading activities to be successive and sustained as much as possible in order to reinforce the story of deception.

It should be noted that the process of deception is a constant one, due to the exchange of information that takes place between the analysis and organisation teams, and the operational ones. However, probably, gathering information about the opponent, analysing and interpreting it can be considered the fundamental actions of the whole operation of misleading. In order to influence the behaviour of the target, it is vital to have help from intelligence structures, and to maintain a constant flow of information on how it perceives the environment, how it processes the information delivered and how it makes decisions, and then analysing the variables in the political, military, economic, social and information environments of the target that can influence it (Field Manual 3-13.4, pp. II-3, II-14).

Another important clarification is how the target perceives, at the cognitive level, the threat and we notice that there is a tendency of individuals to perceive things because of their own expectations, where they are also shaped by context. Their way of thinking can present some vulnerabilities which consist in:

a) the tendency to form hasty reasoning, which can later be changed only by a considerable deliberate psychological effort;

b) assimilation of new sets of information, which may be contradictory, and their use in strengthening the initial reasoning;

c) prolonged exposure to ambiguous or unclear information determines that a subsequent exposure to a new set of information requires a sum of additional information, even if they may be clear from the first moment (Heuer, 1999, pp. 7-14). Although there may be solid evidence that show the inaccuracy of the original reasoning, mental processes make the reorganisation of data and the assimilation of information a difficult task in changing perceptions. Although the dynamics of events indicate other trends, there is an inner resistance of the perception to new changes. Even if the individual is psychologically willing to reanalyse the data and information, the different perspectives he reaches will still be related to the initial reasoning, and cannot be totally changed or eradicated (Ibid., p. 125).

Given these details, the ambiguity of the relationship between information warfare, security intelligence and military intelligence seems to be diminishing. Information warfare is offensive in itself, but it tends to engage actors of their own free will or as victims. As a result, security intelligence needs to adapt to new challenges and respond in a timely manner to threats that, in the current context, are not easy to spot and anticipate. However, the uncertainties of the security environment of the 21st century have led to an expansion of the area of security intelligence, and practically, have led to the narrowing of the boundaries between it and military intelligence. The projection of one state's power on another through information and the deception over the existence or non-existence of significant national capabilities also raises security dilemmas. All this produces perceptions as a result of deliberate actions or as an incalculable effect, but the risk that perceptions will degenerate and turn into fear is very real.

CONCLUSIONS

As we have seen, information warfare, and especially deception, tries to change the perception of individuals in a certain direction. Perception can embody the misunderstanding of a real situation, causing: one state to act hastily in relation to another; a government not to perceive the needs of its own population correctly and to act to its detriment; or the population, influenced by negative feelings and shortcomings, to resort to massive protests against the central authority, up to the civil war. The erroneous perception of a particularly important factor, or a possible or in progress event, can generate unfounded panic and fear, inopportune actions, harmful passivity, disproportionate aggression etc., causing national security problems. In addition, the perception of reality is not a standardised thing, it is different depending on the information that individuals assimilate and interpret, using filters such as personal experience, education, culture, spatial and temporal context, affiliation with a group or a set of rules and specific values etc.

On the other hand, adding the context that hybrid warfare establishes, it causes maximisation of ambiguity on the origin, nature and the initial impact of information and military threat. Corroborated with strategic surprise and deception, there is a risk that decision-makers will be unable to act efficient or could act inopportunely at key moments, as a result of the information flows to which they have been subjected in accordance with their own perceptions. The most relevant example in this regard is the case of Ukraine where the cumulation of military and non-military actions of the Russian Federation led to the annexation of Crimea and the destabilisation of eastern Ukraine (the emergence of armed conflicts in the Donetsk and Luhansk regions), which led to a strategic surprise. Kiev leadership had not foreseen these events and that made it impossible for them to respond in a timely manner.

Because of the changes in security environment the role and relevance of security and military intelligence grow exponentially for two reasons:

a) they can be a source of distortion of information and deception, especially that specialised intelligence institutions have the ability to perform offensive and defensive actions;

b) due to their complexity, they can carry out a wide range of protection measures ranging from strategic objectives to political and military decision-makers who, being part of society, are connected to information flows.

Finally, we can say that technological and theoretical developments and geopolitical evolutions affect the form of concepts of information warfare and security and military intelligence because the dynamics of the security environment emphasise the need for an unexpected, intelligent and surprising approach. Regardless of the state of peace or war and regardless of the target, the combatants (declared or not) will try to obtain, by all means, strategic advantages and gains as an alternative to the direct and mass use of force.

BIBLIOGRAPHY:

1. Clausewitz, von C. (2014). *Despre război*. Editura Antet.
2. Herman, M. (1996). *Intelligence power in peace and war.* Royal Institute of International Affairs.
3. Heuer, J.R.Jr. (1999). *Psychology of Intelligence Analysis*. Central Intelligence Agency: Center for the Study of Intelligence.
4. Kent, S. (1965). *Strategic Intelligence for American World Policy*. Connecticut: Archon Books. Hamden.
5. Molander, C.R., Riddile, S.A., Wilson, A.P. (1996). RAND: *"Strategic information warfare: a new face of war"*.
6. Polyakova, A., Fried, D. (2019). Atlantic Council: *"Democratic Defense against Disinformation 2.0"*.
7. Robinson, P. (2010), *Dicționar de securitate internațională*. Translated by Monica Neamț. Cluj-Napoca: Editura CA Publishing.
8. Shaw, J.E. (2014). *"Military Deception at the Operational Level War"*. The United States Naval War College: Joint Military Operations Department.
9. Theohary, A.C. (2018). *"Information Warfare: Issues for Congress"*. Congressional Research Service.
10. Wardle, C., Derakhshan, H. (2017). *"Information Disorder"*. Council of Europe.
11. AAP-6, *Glosar de termeni și definiții NATO* (English, French and Romanian). (2018). Agenția de Standardizare NATO (ASN).
12. Central Intelligence Agency, *"Deception Maxims: Fact and Folklore"* (1981). Washington: Office of Research and Development.
13. Clark, M.R., Mitchell, L.W. (2019). *Deception. Counterdeception and Counterintelligence*. Washington D.C.: CQ Press.
14. Department of Defense (DoD) (US), *Dictionary of Military and Associated Terms*. (2020). Joint Publication (JP).
15. Field Manual 3-13.4, *Army Support to Military Deception* (2019). Washington: Headquarters, Department of the Army.

INTELLIGENCE CHALLENGES AT THE EUROPEAN UNION LEVEL

Colonel Robert CĂLINOIU, PhD Student
EU Military Staff

Colonel (r.) Prof. Dănuț-Mircea CHIRIAC, PhD
"Carol I" National Defence University, Bucharest

Since its creation in 1950, as an organisation of states sharing primarily economic interests, the European Union (EU) has been developed continuously on multiple levels, the security and defence domain being one of the most dynamic starting in 2000. Therefore, in 2001, there were established the Political and Security Committee – PSC, the EU Military Committee – EUMC, and the EU Military Staff – EUMS – within the General Secretariat of the EU Council. Eventually, after the creation of the European External Action Service (EEAS) in 2009, EUMS has changed the subordination to this structure.

One of the five directorates of EUMS is the Intelligence Directorate – DINT whose mission is to provide strategic intelligence to its customers.

Along the process of developing and improving the intelligence activity, in 2007 the EEAS leadership made the decision of creating the Single Intelligence Analysis Capacity – SIAC, bringing together the military expertise of DINT and the civilian intelligence knowledge of the EU Intelligence Centre (INTCEN).

Since its inception, DINT has proved to be a very effective fusion centre of the national intelligence products, issuing strategic documents of significant interest for the EU and national leaders alike, and positively influencing the EU and member nation's security. Nevertheless, the importance of a flawless functioning of DINT and SIAC results not only from its successes but also from failures, which could have had a major impact on the security of some European states or at the EU level. One of this is the shot down of the Malaysia Airlines Flight 17 (MH17) over the Ukrainian airspace, whose case study we will present in the present article.

Keywords: security;defence; European Union; military/civilian defence information; strategy;

INTRODUCTION. SHORT HISTORY OF THE ESTABLISHMENT OF THE DEFENCE STRUCTURES WITHIN THE EUROPEAN UNION

The European cooperation initiatives in political and economic domains have their origins after the end of the Second World War. After discussions in bilateral and multilateral formats, in 1948 the Western European Union – (WEU) was created by the Great Britain, France, Belgium, West Germany, Italy, Luxembourg, and the Netherlands. This format permitted consultations on various subjects of common interests, mainly political and economic, but also on European security and defence. The Treaty of Maastricht, becoming one of the cooperation pillars within the European Union, introduced the concept of Common Foreign and Security Policy (CFSP) starting 1993. The Treaty affirmed that *"the common foreign and security policy shall include all questions related to the security of the Union, including the eventual framing of a common defence policy, which might in time lead to a common defence" (Treaty of Maastricht, Title V, art J 4)*.

After five years, during the Franco-British St. Malo Summit (4 December 1998), the British Prime-Minister, Tony Blair, and the French President, Jacques Chirac, signed a joint declaration stating that *"the Union must have the capacity for autonomous action, backed up by credible military forces, the means to decide to use them, and a readiness to do so, in order to respond to international crises" (Joint Declaration issued at the British-French Summit, 1998, Art. 2)*. The declaration signalled a significant change in the UK stance on security and defence, from blocking any intention of creating military structures within the EU to an open agreement. At the same time, France, that withdrew from NATO's military structures in 1996 (reversing its position in 2009), was seeking means to consolidate its security within the European Union.

The Joint Declaration allowed the European States to launch, during the European Council in Koln (June 1999), the concept of *European Security and Defence Policy – ESDP*, and at the end of next year, through the Treaty of Nice, to create the legal basis for European cooperation in the field of security and defence by defining the competencies, structures and means necessary to develop a Common Security and Defence Policy (CSDP).

To the creation and development of the formal structures having as tasks the CFSP and CSDP fields contributed, along with the progressive accumulation aforementioned, the security situation in Europe. This had been characterised by the wars in the Former Republic of Yugoslavia, the disintegration of the Soviet Union and the appearance on its territory of a number of independent states, as well as the increasing number of the terrorist attacks by foreign perpetrators on European soil. The main goal of CSDP has been the management of the crisis outside the EU's territory, objective leading to the creation in 2001 of the following entities: the Political and Security Committee (PSC), the EU Military Committee (EUMC), and the EU Military Staff (EUMS) – within the General Secretariat of the Council.

The EU Council decision stated that, in the field of intelligence, the Military Staff is to perform early warning, situation assessment and strategic planning for missions and tasks referred to in Article 17(2) of the TEU, including those identified in the European Security Strategy.

After the signing of the Lisbon Treaty in 2009 and the establishment of the European External Action Service (EEAS), all CSDP structures, including EUMS, moved from the General Secretariat of the Council to the newly created EEAS. To underline the importance of EUMS as a single source of military expertise within the EU institutions, it was subordinated directly to the High Representative/Vice-President of the European Commission (HR/VP).

SHORT HISTORY OF THE ESTABLISHMENT OF THE INTELLIGENCE STRUCTURES WITHIN THE EUROPEAN UNION

One of the components of the EUMS is the Intelligence Directorate (EUMS Intelligence Directorate – DINT), established in 2001, at the same time as the parent organisation. Its missions include providing intelligence on the political strategic level as well as in support for EU operations and missions, providing a timely and accurate situational awareness and the intelligence input to crisis response planning and assessment for military operations, civilian missions and exercises (EU Council Decision, 2001). The personnel coming from the member states defence intelligence organisations (DIO) as National Seconded Experts (SNEs) for a period not exceeding four years are staffing DINT. Each member state's DIO has a point of contact (POC) within DINT providing the two-way channel of communication and transfer of intelligence products. DINT has no collection means, the classified intelligence coming from the parent DIOs or from the civilian intelligence organisations – CIO (the later via the Intelligence Centre – INTCEN), a civilian structure with whom DINT works closely within the Single Intelligence Analysis Capacity (SIAC) format. A third source of intelligence is the EU Satellite Centre (SATCEN), which is providing products derived from imagery acquired upon request. DINT is also benefiting of information coming from the EU Delegations in various states, gathered by its personnel during

the Fact-Finding Missions (FFM) from Think Tanks or by participating in conferences and seminaries having subjects of interest (ongoing or potential crises areas). The inputs from DIOs or CIOs are submitted on a voluntary basis, having subjects connected with areas or topics of immediate interests for a certain member state (crisis, terrorism, illegal migration etc.) (Ibid., p. 6, point a).

The Production Branch is organised in geographical and subjects sections (transnational and hybrid threats). Its products are delivered in written format or oral briefs, planned or upon EU leaders' request. Among the issued documents, there are Intelligence Briefing Notes, Threat Assessments, and Intelligence Assessments. Periodical issued intelligence products are Annual Global Threat Review – AGTR, and SIAC Weekly.

The management of the intelligence domain is performed, from the member states' DIOs perspective by the Board of Directors (BoD), composed by the directors of the military intelligence services from EU member states. BoD convenes once a year, or as many times as situation requires. In order to prepare the BoD meeting, two other working groups take place, at the Directors for Analysis and the Plans and Policy Directors.

On the civilian side, in 1999, it was created the Joint Situation Centre (SITCEN, having the mission to produce open source analysis (OSINT). In 2002, SITCEN becomes a forum of exchanging classified information between itself and seven EU member states (France, Germany, Italy, The Netherlands, Spain, Sweden, and Great Britain).

SITCEN grew progressively by accepting more member states' civilian intelligence organisations, eventually becoming (2012) the Intelligence and Analysis Centre (INTCEN), a civilian intelligence organisation at the level of the general directorate within EEAS, under the direct subordination of HR/VP, and the main DINT partner within the SIAC format.

INTCEN has two main divisions, the Intelligence Analysis Division and the Open Source Research and Support (OSINT) Division (Impetus, 2019, p. 10).

The Intelligence Analysis Division covers both the regions of major interest for the EU CFSP/CSDP according to the 2016 EU Global Strategy, and the subjects of concern for EU' security like counterterrorism, non-proliferation, migration, energy security, cyber and hybrid threats. Unlike DINT, INTCEN benefits by EU carrier employees, beside the National Seconded Experts coming from the CIOs of the member states.

In order to better inform the leadership on the growing hybrid threats directed at the EU, in 2016, DINT and INTCEN created the Hybrid Fusion Cell, with experts from the two structures. The Hybrid Fusion Cell analyses matters like disinformation, cyber-attacks, psychological operations (psyops), subversive actions, terrorism, sabotage, exploitation of the cultural, language or religious divisions, illegal economic activities directed to attain political advantages (*"pipeline politics"*), support for secessionist movements, migration and migrants exploitation, use of mercenaries and third parties in covert actions (Barber et al.).

EU Satellite Centre (SATCEN) is also an important part of the intelligence architecture of the European Union. Established in 1993 under the name of Western European Union Satellite Centre, it has functioned under the current designation since 2002. Operationally coordinated by the EEAS, SATCEN provides early warning of potential crises and imagery products on the customer's request, the main beneficiaries being DINT and INTCEN. Other EU organisations, like EUROPOL, FRONTEX, Civilian Planning and Conduct Capability (CPCC) are among its customers, as well as the EU member states. Its products are based on the exploitation of spatial and aerial capabilities (GEOINT and IMINT), corroborated with collateral data from OSINT or Social Media Intelligence (SOCMINT) (Salmi).

EU INTELLIGENCE SUPPORT ARCHITECTURE AND THE WORKING RELATIONSHIPS OF ITS INTELLIGENCE STRUCTURES

In 2012, after the establishment of the EEAS and taking into account the growing threats of the security environment, the HR/VP issued the decision of founding the EEAS Intelligence Support Architecture – ISA (Impetus, Ibid., pp. 10-11).

The main goal of ISA has been to take into account all relevant developments and design an intelligence support package – to define responsibilities, provide direction and guidance, and create provisions for effective production and fast, secure and reliable dissemination of intelligence products to the EU decision-makers and member states. The ISA also includes provisions on coordination and liaison with the MS intelligence organisations, European Commission and with international organisations.

The above-mentioned HR/VP Decision defines *"intelligence"* as information that has been collected, processed and disseminated for the use by decision-makers and other customers and ISA as structures, processes and activities related to intelligence. It aims to optimise the intelligence function within the EEAS and encourages close cooperation and coordination across EU institutions and between intelligence stakeholders.

ISA included in 2012 two central structures – the Intelligence Steering Board (ISB), transformed in 2019 by a new decision issued by the HR/VP, Josep Borrell, Intelligence Policy Board (IPB), and Intelligence Working Group (IWG). EU INTCEN and DINT provide jointly the Secretariat function for both ISB and IWG. The ISB defines intelligence requirements and priorities at the strategic level as well as endorses structural, organisational and policy measures required to improve the Architecture. It also provides guidance to address deficiencies in the field of security. The HR/VP or EEAS Executive Secretary General (ESG) chairs the Board.

The IWG further defines, specifies and adjusts EEAS intelligence requirements and priorities. In particular, it proposes the strategic intelligence direction and Prioritised Intelligence Requirements (PIR) for the intelligence. The IWG synchronises the tasking of the Single Intelligence Analysis Capacity (SIAC), defines SIAC product range, develops and monitors a feedback mechanism. The IWG is co-chaired by the Director EU INTCEN and Director EUMS INT.

The establishment of the Single Intelligence Analysis Capacity – SIAC was possible due to the development by the former Secretary General/High Representative (SG/HR) Javier Solana of the concept of Comprehensive Approach to the external crises and conflicts.

The idea at that time was to bring together, in a functional way, analytical capacities from both the EU Situation Centre (EU SITCEN, now renamed EUINTCEN) and DINT, thus benefiting from a wide EU knowledge base for producing enhanced and reliable intelligence. This resulted in the SIAC arrangement initiated by directors of EUMS and EU SITCEN at the beginning of 2007. In addition, and in line with the Comprehensive Approach concept, the EU intelligence community intensified its efforts to widen the scope of access to and utilisation of all the information and data already available within the EU.

SIAC has become one of the EU forerunners in the field of producing synergies by a joint civilian-military approach, providing high valuable intelligence to the EU and member states. The creation of EEAS and the transfer of EUMS and INTCEN to it has led to a significant increase of demand for specific products and, accordingly, the tasks multiplied.

In the SIAC format is taking place the sharing of intelligence received from DIOs and CIOs through the secured national channels, the PIR issued by IPB are detailed and answered, joint task forces mixing the military and civilian intelligence expertise are created to tackle various subjects of interest. One of the successful examples is the Hybrid Fusion Cell, created to analyse the specific threats directed against the EU interests and providing intelligence in this new field of security.

SIAC intelligence products are disseminated to EU decision-makers and DIOs and CIOs of the member states, from this viewpoint SIAC working as an Intelligence Fusion Centre. The advantage of this format resides in the sharing of expertise from one member state to another on subjects of temporary interest (new crises, mission preparation, specific training).

In addition, SIAC organises working groups where experienced analysts from CIOs, DIOs, international partners (NATO) or Non-Governmental Organisations (NGO) participate and share their knowledge on different topics of interests in common benefit of participants. Moreover, within SIAC there are formed joint teams for Fact Finding Missions (FFM) in areas of concern.

To meet all these challenges, further systemic transformation is needed. At this stage, it is essential to revise and optimise processes, change the information sharing intelligence culture within the EU, adopt suitable technology and adjust the conceptual approach to the intelligence support function. In short, promote intelligence within the EU, as well as produce intelligence for the EEAS with a more operational and dynamic approach.

INTELLIGENCE CULTURE WITHIN THE EU – MAJOR VULNERABILITY IN COUNTERING THE THREATS AND DIMINISHING THE RISKS

The culture particular to the intelligence domain at the European level is in its early stages of development due to a series of factors. First, it is the continuing transformation of the EU, now comprising of 28 members after reaching its peak of 27, each having its own interests, identities, similar but not identical security cultures. Equally important, the defence and security domains are in the national responsibility (Treaty on European Union and Treaty on the Functioning of the European Union, Title I, Art. 4, Para. 2), the European policies in this fields having to harmonise diverse interests and particular approaches. The decisions in the security and defence fields have to be taken by consensus. Member states' policies are usually based on the national intelligence inputs, grounded on information acquired proportionally with the resources available, internal priorities (focus on crisis in their proximity) and thus incomplete or biased.

The consequences of this reality at the EU level are difficult mediation of interests, unnecessary multiplication of efforts (financial or human) for the same identified threat (e.g. illegal migration or terrorism) or the lack of a common strategy to counter transnational threats.

Not least, a major impediment in the development of a European intelligence culture is the lack of appetite of the member states to create common independent intelligence structures having all the necessary means for collecting, processing and delivering relevant intelligence products to all customers, EU institutions or member states. The lack of solid EU intelligence structures efficiently working in the benefit of EU's security and defence, and becoming renown over time, has a major impact in maintaining the current culture where the written classified information generates more administrative concerns than benefit on subjects of strategic interest.

The lack of timely information and the slow adaptation of the structures to the current challenges represent also aspects that should be addressed in order to increase the profile of the intelligence within the EU. The illegal migration and its associated facets (terrorism, organised crime), which caused a major threat to the security of the EU and a long debate among the member states, was perceived very late as a threat of a strategic level. The cyber threats promoted by entities difficult to detect are also countered with insufficient means at the EU level, the centre of gravity resting on the nations, while the modus operandi is by definition international.

Using proxies in a foreign country for attaining military, political, and economic goals is a strategy more and more used and causing difficulties in being countered by the democratic states and organisations using the existing legal means. While the sponsors are easy to detect, the lack of instruments to counter this strategy leads to protracting conflict and crises generating regional instability and security challenges to EU. Without a proper security, the criminals are using the fundamental rights like the freedom of movement to challenge the EU's security and its citizens wellbeing. The terrorist attacks in Madrid, Paris, and Brussels are the most notorious examples of this kind. The cyber-attacks or phishing attempts against EU institutions request a decisive riposte from a solid defence system.

Changing by force the borders of states thus affecting the security in the EU's proximity (Crimea), influencing the free and democratic elections by third parties using illegal means, manipulating the national referendums having a direct and significant impact on EU's existence (BREXIT), disinformation campaigns in EU member states concerning the EU's institutions policies and actions, encouraging the secessionist movements and radicalism are examples requiring strong EU intelligence institutions capable of providing early warning, detecting and timely countering such actions.

Finally, yet importantly, a well-timed and adequate reaction to a military crisis in the close neighbourhood of the EU could raise the awareness of the population and avoid dramatic consequences to the security of the Union and its citizens. Such an example will be analysed in the case study below.

CASE STUDY ON THE SHOT DOWN OF THE MALAYSIA AIRLINES FLIGHT MH17 (MH17) OVER THE UKRAINIAN AIR SPACE. LESSONS LEARNED

Case studies concerning successful operations or major failures with strategic impact have been, throughout history, a preoccupation for the professionals demotivated by the chain of command (Plame, 2007, p. 8), academics looking for improving the field (Ibid.), or visionary leaders wanting to help their successors repeating the same mistakes (Bush Jr., 2010, Powell, 2003, Rice, 2011).

In analysing the failures, two main situations are described. First, ignoring or diminishing the importance of relevant indicators concerning a possible course of action, which proves in the end to be unfavourable to own interests. The second is the one of a correct and timely analysis presented by the intelligence services to the decision-maker, without being capable of convincing the later to act accordingly and avert the negative consequences (Wirtz).

The necessity to study the intelligence failures and extract useful lessons goes back in the past and is always a requirement in order to avoid repeating the same mistakes. Nowadays, when the technology allows the fast access to knowledge and rapid exchange of information and it is more and more difficult for one state to attribute hybrid or asymmetric actions to a certain entity without cooperating with a wide array of other organisations, learning from mistakes is essential. Analysing the techniques, tactics and procedures in the cases of killing of political opponents on the soil of EU states, melding in the elections of foreign states perceived as enemies, cyber-attacks of critical infrastructure for intimidation or economic advantages is mandatory in order to defend the security of a nation or alliance. Studying the favourable conditions leading to this kind of attacks, like prolonging the stay in power of authoritarian leaders with expansionist visions in pseudo-democratic states and dismissing the international rule of law in favour of the rule of the most powerful may provide the right tools and measures against the villains. Difficult to attribute, the asymmetric attacks escape from the classical definition of an armed aggression of the UN Charter[1] and the eventual tailored, lawful international punishment following a resolution in the UN Security Council. The failure in taking adequate measures, other than weak economic sanctions against persons and countries, or blaming them at international conferences encourages the perpetrators to repeat the deeds. In these circumstances, it is even more demanding for the intelligence services to perform early warning, counter such hostile actions and this could be done only by analysing and offering efficient solutions to the current challenges.

The events

The crisis in Ukraine erupted on 21 November 2013, when Ukrainian citizens starting protesting in the capital city of Kiev against the President Victor Yanukovych following his decision to reject a project for e greater economic European integration of Ukraine. The protesters gathered in the Independence Square being met with force by the regime, which led to a rapid increase of their number. Determined in expressing their demands, the demonstrators soon renamed the Independence Square as Euromaidan (European Square).

The protest progressively escalated, eventually leading to an armed confrontation. In the timeframe of 18 to 20 February 2014 the battle between the camps resulted in approximately 130 deaths, among which 18 were members of the security forces. Being clear that a national reconciliation was not possible without an international involvement, the EU and the Russian Federation helped reaching an Agreement, signed on 21 February 2014 (Kariakina et al.). However, for unknown reasons, the Russian Federation representative refused to sign the document at the last moment. The failure of mediation and the violent escalation of the conflict led to the ousting of the president Victor Yanukovych and the takeover of power by a heterogeneous group of people.

Taking advantage of the crisis developments and the power vacuum, in March 2014, the Russian Federation troops stationed in Crimean Peninsula due to a bilateral agreement between the two countries (Partition Treaty), and special forces troops without identification badges, deployed earlier, started taking over progressively the Ukrainian bases and the Crimean Peninsula territory.

In order to politically formalise the hostile takeover, in the occupied territory it was organised a referendum on which the citizens had to choose Crimea's integration within the Russian Federation or the return to the provision of the 1992 Constitution and being part of Ukraine. The results of the referendum (contested at the international level) showed the supposed will of the majority of the population (96.77% of the votes from an 83.1% turnover) to become a part of the Russian Federation (Russia Today, 2014).

Subsequently, motivating that the rights of the Russian citizens and Ukrainians of Russian origins had to be protected in South-Eastern Ukraine, secessionist movements from Donetsk and Luhansk regions organised similar referendums, declaring the Popular Republics on both regions.

The statements of independence of separatists in the two aforementioned regions led to transforming the ethnic divergences in armed conflicts between the Ukrainian security forces and the local paramilitary backed by covert Russians military capabilities (Anders Fogh Rasmussen, Speeches & Transcripts, 2014). On this overall dissolution of the state authority, combined with classical war tactics, psychological warfare, and hybrid actions, the shot down of the Malaysia Airlines Flight MH17 (MH17) over the Ukrainian air space (Hrabove) took place.

[1] Article 51, UN Charter, states: *"Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security".*

MH 17 took off from Amsterdam to Kuala Lumpur on 17 July 2014. The flight route of the planes from Amsterdam to Kuala Lumpur routinely passed over the Ukrainian territory, precisely over the Donetsk region where an armed conflict involving high calibre armament, including ground to air artillery was used. Even though there was information that artillery systems capable of shooting down an airplane flying over 10,000 meters[2] were in the hands of the separatist forces, either sized from the warehouses of the Ukrainian Armed Forces or received from friendly entities, the flight restrictions (Notice to Airmen – NOTAM) in place concerned only flights below 9,700 meters, and not the complete interdiction of flights over the war zone. Indeed, various media reports[3] indicated in June that a missile launcher system BUK-M1 has been sized and repaired by the separatists[4], while the transfer of different military capabilities by the Russian Federation over the border in the secessionist regions was common knowledge.

At approximately 15.20 (Central European Time – CET) MH 17 disappeared from radars in the Hrabove area and the communication of the Ukrainian Air Traffic Service with the plane had been lost. Even though it was not clear immediately what happened, separatists radio communications indicated their belief that they succeeded in shooting down a military Ukrainian plane AN-26[5]. Four days after the crash, the United Nations Security Council unanimously adopted Resolution 2166, expressing support for an independent international aviation investigation into the crash.

The official report that followed, issued by the Dutch Safety Board[6], arrived to the conclusion that the in-flight disintegration of the plane near the Ukrainian/Russian border was the result of the detonation of a warhead. The weapon used was a 9N314M – model warhead carried on the 9M38-series of missiles, as installed on the Buk surface-to-air missile system.

It is worth mentioning that, in one week before the crash of the MH 17, 888 flights passed over the same territory facing the same security risks, unidentified by any national and international entity, military or civilian.

[2] According to the official data, the Boeing 777 was flying at an altitude of 10,100 meters; https://libraryonline.erau.edu/online-full-text/ntsb/miscellaneous-reports/mh17-crash-en.pdf, retrieved on 18 October 2020.

[3] On 6 June 2014, *The International New York Time.*

[4] On 11 June 2014, *Argumenty nedeli.*

[5] On 14 June 2014 the separatists shot down an IL-76 airplane belonging to the Ukrainian Air Forces, while landing at the Luhansk International Airport, causing the death of 49 soldiers; on 14 July 2014 the separatists shot down an AN-26 airplane belonging to the same Ukrainian Air Forces flying at an altitude of 6,500 meters, claiming on social media that the success was possible due to the use of a Buk-M1 surface-to-air missile system seized from the Ukrainian Armed Forces and operationalised by own efforts; https://libraryonline.erau.edu/online-full-text/ntsb/miscellaneous-reports/mh17-crash-en.pdf, retrieved on 18 October 2020.

[6] The Dutch Safety Board official reports in English can be accessed at https://www.onderzoeksraad.nl/en/page/3546/crash-mh17-17-july-2014, retrieved on 18 October 2020.

Lessons learned

One of the favourable courses of action would have been, from the intelligence services perspective, that through a flawless tradecraft, the mass-media reports concerning the existence in the hands of the separatists of a military capability able to shot down a plane flying at a high altitude (over 10,000 meters) had been verified via intelligence means, double-checked by military analysts and confirmed or infirmed with a sufficient degree of accuracy thus permitting the eventual transmission of an intelligence product to the decision-makers.

Corroborating the technical data of the surface-to-air systems existent in the area, with the information concerning the recent shooting down of other planes, the constant transfer of military capabilities over the Russian/Ukrainian border, and taking into consideration the asymmetric war characteristics of continuous disinformation, lack of proper training, and the disrespect for the laws of war, a thorough analysis could have reached to the conclusion that the risks posed to the civil aviation are greater than the economic benefits and the comfort of following a known flying pattern.

Another positive course of action would have been the sharing of national pieces of intelligence related to the armed conflict with the European Single Intelligence Analysis Capacity, which could have acted as a fusion centre putting the pieces together and adequately informing the EU institutions and decision-makers, and the EU member states and partners about the security risks. As such, the European Union Aviation Safety Agency (EASA) would have received a useful intelligence product and issued a warning to the European air operators, furtherly informing the International Civil Aviation Organisation (ICAO), which has the duty of issuing NOTAM at the international level.

An additional element, which could have helped avoiding the tragedy, could have been a better cooperation of the Ukrainian security/intelligence institutions with the European counterparts, especially taking into consideration the existence of similar cases even though involving flights at a lower altitude (under 7,000 meters). Closing completely the air space in the conflict area, a national responsibility, would have been a salutary preventive measure, in consensus with the national and international security policies, and more important saving the lives of the 298 citizens from 10 countries.

The failure in preventing the shooting down of the flight MH 17 showed how a regional conflict, insufficiently monitored and analysed, may have major consequences upon the security of the European and international citizens.

Moreover, such an event has the potential of inflaming an existing armed conflict, if among the passengers killed would be citizens with a high political or social profile belonging to states having a high capability of military retaliation and authoritarian leaders in search of global recognition of their power.

The European attentiveness in monitoring the Ukrainian armed conflict and avoiding such tragic situations had to be far greater, as the Ukrainian crisis had started following the strong will of the majority of its citizens for a greater cooperation with the EU – a political, economic, security, and social role model.

BIBLIOGRAPHY:

1. Lt Col Berbel-Lopez, F.R. (EUMS) (2018). CSDP Course presentation, course organised by the European Security and Defence College, in cooperation with the national Defence University, Bucharest.
2. Bush, G.Jr. (2010). *Decision Points*. New York: Crown Publishing Group.
3. Kariakina, A., Sergatskova, K., Kakhidze, A. (2017). *The Maidan Cases in Numbers and in Pictures*, https://en.hromadske.ua/posts/the_maidan_cases, retrieved on 27 September 2020, corroborated with the Amnesty International documents, https://www.rferl.org/a/ukraine-maidan-justice-victims-amnesty-fifth-anniversary/29779358.html, retrieved on 27 September 2020.
4. Lassche, D., *Militaire Spectator*, https://www.militairespectator.nl/thema/internationale-samenwerking/artikel/eu-militarystaff-frog-boiling-water, retrieved on 12 August 2020.
5. Plame,V. (2007). *Fair Game: My Life as a Spy, My Betrayal by the White House*. New York: Simon and Schuster.
6. Powell, C. (2003). *My American Journey*. New York: Ballantine Books.
7. Rasmussen, A.F Speeches & transcripts; *Secretary General sets out NATO's position on Russia-Ukraine crisis*, https://www.nato.int/cps/en/natolive/opinions_110643.htm, retrieved on 27 September 2020.
8. Rice, C. (2011). *No Higher Honor: A Memoir of My Years in Washington*. Random House Audio.
9. Salmi, I., former INTCEN Director, interview in *Moondial Nieuws*, Belgium, https://www.mo.be/en/interview/ilkka-salmi-eu-s-007, retrieved on 13 September 2020.
10. Wirtz, J.J. (2001). *Intelligence to Please? The Order of Battle Controversy During the Vietnam War*. Political Science Quarterly.
11. EUMS Information Brochure, https://www.cvce.eu/en/obj/information_brochure_on_the_european_union_military_staff_eums-en-1bcbd497-c5e3-4b7a-ab54-9e392e0c1483.html, retrieved on 13 September 2020.
12. Council Decision 2001/80/CFSP on 22.01.2001, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:r00006&from=EN, retrieved on 13 September 2020.
13. Joint Declaration issued at the British-French Summit Saint-Malo, https://www.cvce.eu/content/publication/2008/3/31/f3cd16fb-fc37-4d52-936f-c8e9bc80f24f/publishable_en.pdf, retrieved on 3 August 2020.

14. Dutch Safety Board Reports, https://www.onderzoeksraad.nl/en/page/3546/crash-mh17-17-july-2014 and https://libraryonline.erau.edu/online-full-text/ntsb/miscellaneous-reports/mh17-crash-en.pdf, retrieved on 23 September 2020.
15. *Impetus* Review, EUMS, no. 17 spring/ summer 2014, http://www.eeas.europa.eu/archives/docs/csdp/structures-instruments-agencies/eu-military-staff/images/impetus_springsummer_14.pdf, retrieved on 3 August 2020.
16. Idem, no. 28, autumn/winter, 2019, https://eeas.europa.eu/sites/eeas/files/eums_impetus_28_final_web.pdf, retrieved on 13 September 2020.
17. Official EEAS website, https://eeas.europa.eu/headquarters/headquarters-homepage_en/3602/Organizationchart, retrieved on 23 August 2020.
18. *Treaty on European Union*, Title I, Art. 4,https://europa.eu/european-union/sites/europaeu/files/docs/body/treaty_on_european_union_en.pdf, retrieved on 13 September 2020.
19. Treaty of Maastricht, Title V – *Provisions on a common Foreign and Security Policy*, https://europa.eu/european-union/sites/europaeu/files/docs/body/treaty_on_european_union_en.pdf, retrieved on 13 September 2020.

THE INFLUENCE OF MIGRATION ON SOCIETAL SECURITY IN THE EUROPEAN UNION

Delia-Mihaela MARINESCU, PhD Student

"Carol I" National Defence University, Bucharest

The complexity and globalisation of migration are normal processes of functioning and evolution of contemporary European society, currently facing the COVID-19 pandemic that will exacerbate existing security risks by imposing on member states and the North Atlantic Alliance important integral decisions related to both the humanitarian crisis of refugees correlated with the provision of public health measures and their economic and social impact on social security.

There is a constant evolution of the issue of international migration within the EU, but also a concern for permanent improvement of its legal framework, migration bringing both benefits and costs for the area of freedom, security and justice of the EU.

In fact, migration is a fundamental threat to the cohesion and identity of society, the fundamental components of societal security. A concept developed by the "Copenhagen School", migration can be considered the main source of societal insecurity as it can threaten society's identity and change its composition.

Keywords: migration; societal security; legislation; European Union; mobility;

INTRODUCTION

An essential principle of community building, *freedom of movement* is one of the four fundamental freedoms enshrined at European level (Beșteliu, Brumar, 2010, p. 79). Although, initially, in 1957, in the *Treaty establishing the European Economic Community*, the free movement of persons was linked to the need to find a job in another state, European regulations guaranteeing a legal status only to migrant workers, later the scope of this concept became much wider, in 1992, through the *Treaty on the European Union (TEU)*, and in 2007, through the *Treaty on the Functioning of the European Union (TFEU)*, taking into account both the extended protection granted to the family members of the migrants and the various reasons underlying the decision to change the state of residence.

The importance of the migration phenomenon and the impact on the societal security of the European Union results from its complexity and from the implications it creates both at legislative level, through the need to adopt an effective normative framework in order to control migration and ensure a legal status capable of providing rights to migrants in the host state, as well as at the social and cultural level.

Currently, international migration is a real link between the member states of the European Union and with third countries, the phenomenon of globalisation having a decisive role in increasing migration.

If in the first treaties of the European Community there were different legal regulations in European states, which made migrants subject to the legal rules of the host state, with the creation of the European Union, unitary policies were adopted, applicable at the level of all member states.

In this context, the European Union adopts unitary measures to manage migratory flows in order to preserve cultural diversity and manage multiple challenges, while ensuring respect for the universal nature of human rights (Corlățean, 2012, p. 14). Thus, the analysis of the migration phenomenon, as a threat to the societal security of the European Union must be related to the evolution of community building as well as of the member states, taking into account the particular aspects of the society in which migrants live and work.

The complexity of the migration phenomenon determines the decision-makers to adopt measures in the field depending on the policies of the European Union, of the member states, but also on ensuring all the rights of migrants.

Although, traditionally, European regulations are comprehensive, they must be able to ensure the implementation of general principles leading to migration control, but also to combating illegal migration. These measures can be ordered only through effective international cooperation.

THE INFLUENCE OF MIGRATION ON THE LABOUR MARKET

Migration is the main source of labour force shortages in migrants' countries of origin. Thus, from the perspective of employers, the departure of labour force is a barrier in the economic development of certain regions, affecting the level of development of those areas, which is materialised in the inability to fully meet market requirements, by reducing production capacity.

Most migrants decide to leave their country of origin in general for financial reasons, to find a better paid job or to develop professionally, to ensure a better standard of living for the whole family.

The problems that determine migration are based on the low level of wages, the proliferation of undeclared work in certain sectors of activity, such as construction, and the lack of qualification to perform a certain activity.

Although references to migration have traditionally referred to the external dimension of this phenomenon, internal migration, which also has a strong impact on national and zonal security, must not be neglected.

In this context, bringing in foreign citizens to work in certain areas where the demand for labour is higher has much wider effects, by involving more states, so it is preferable for employers to initially focus on finding solutions within the same region in order to fill the staff deficit and subsequently on trying to hire emigrants. This possibility would have a lower impact in the social sphere, regarding the family life, in the conditions in which the international migration represents a strong disturbing element of the private life, by breaking the family ties.

Despite the fact that in many branches of activity the technological development tends to reduce the human deficit, the lack of personnel is a destabilising factor of the labour market.

It is also worth noting that employment is preferred to metropolitan areas to the detriment of underdeveloped regions, given the multitude of opportunities and the variety of areas in which a person with a clear qualification can find a job.

The benefits of migrants to the European Union as a whole must not be strictly related to economic progress and labour market benefits, but also to taking into account the social issue of integrating migrants in European countries, respecting the diversity, traditions and culture of the countries of origin, especially in the conditions in which migration is a reversible phenomenon, which can no longer be considered unpredictable.

Although in most cases, the labour market is viewed only from the perspective of finding a job, it is essential to address the educational issue, mainly the constant qualification for a certain job, especially in the context in which most migrants are young people looking for personal and professional development amid the lack of real employment opportunities in their home state.

Thus, it is noted that migration should not be reported exclusively to unskilled workers, but also to people who choose to improve their professional training in another state and occupy positions of high responsibility that involve a high degree of knowledge in the field, so it is of great importance is the recognition of qualifications and diplomas obtained in other states.

Closely related to the evolution of the migration phenomenon, discrimination must be analysed in the conditions in which migrants are often victims of factual and legal inequalities, but also of stereotypes, being difficult to accept them in certain social circles on the grounds of origin.

By virtue of respecting the principles of equal treatment and non-discrimination, which are universally recognised (Muscalu, 2015, p. 289), the legal status of the different categories of migrants must be the same, regardless of the reason for the decision to work in another state; at the same time, migrants must have equal privileges with the citizens of the destination state, regarding the promotion possibilities, the general working conditions and the salary to observe the fundamental objectives of the International Labour Organisation, which aim to ensure equal opportunities for all employees (Ștefănescu, 2010, p. 672) as well as to respond to the need to protect fundamental human rights (Tofan&Petrișor, 2013, p. 14).

Labour force migration is a normal process for any democratic society, being absolutely indispensable for the smooth running of economic progress, being an opportunity for citizens of less developed countries. That is why the general trend is to migrate to areas with better industry, with more permissive social protection systems, which provide real premises for integration in the professional sphere as well as in social life.

THE IMPACT OF MIGRATION ON SOCIETAL SECURITY IN ROMANIA

Traditionally, Romania is not a host state, but a gateway to other European areas. From the statistics made in Romania (Peticilă, 2019), it turns out that the number of men leaving the country is higher than that of women, being generally young people who come from underdeveloped areas and who are looking for a better standard of living.

In this context, from a demographic point of view, the perspectives regarding the evolution of Romania show an aging trend of the population left in the country and the creation of an imbalance at the level of society, which doubled by economic difficulties in certain sectors, can affect security, all the more the number of immigrants in Romania is, according to statistics, 8.9 per 1000 inhabitants at the level of 2018 (National Institute of Statistics, Romania).

As in the European Union, in Romania, the management of migration issues is a challenge to state security both by the danger created on the cohesion of society and by affecting the cultural identity created by the departure of a large number of citizens to other states. Certainly Romania, as a full member state of the European Union, must have an approach to migration and societal security in accordance with European standards in the field, supporting the efforts of the European Commission to develop and implement a collective policy in terms of migration management and border security, for the effective monitoring of the EU Regional Trust Fund in response to the Syrian crisis, with regard to health care and education to prevent loss of life and criminal activities of migration, to be actively concerned about the incipient nature of supporting labour market integration and employment opportunities for refugees, in the context of the labour market changes generated by the European Union's plans to combat climate change, the policy of promoting the circular economy and the digital society, to develop ways to consult and inform the population regarding the preparation of waste and water management infrastructure projects in hotspot areas, as an environmental protection measure in hotspot areas that face the greatest pressure of the migration phenomenon (Decision no. 24/8 September 2020).

Romania and the European Union cannot remain indifferent to humanitarian tragedies related to migration that occur within the member states, such as the fire on 9 September 2020 that burned the Moria refugee camp from the Greek island of Lesbos, a camp where there were about 12,600 refugees and migrants, given that the location has a capacity of only 2800 people (Deutsche Welle). In addition, considering the quarantine because of the coronavirus outbreak, the existence and the way of managing this camp permanently produced the dissatisfaction of the locals.

The Moria tragedy hastened the adoption, on 23 September 2020, of the European Commission's proposal to implement the new *"European Pact on Migration and Asylum"* (EU Official Journal, 2020), which proposes changing the rules on asylum and migration by establishing efficient and faster procedures in the asylum and migration system and ensuring a balance between the principles of fair sharing of responsibility and solidarity for restoring confidence between member states and the European Union's capacity to manage migration.

This new pact provides for the introduction of an integrated border procedure that includes, for the first time, pre-entry verification, which involves establishing the identity of all persons who cross the EU's external borders without permission or who have landed as a result of search and rescue, performing medical and security checks, fingerprinting and registration in the Eurodac database (ESO, 2020). Each member state must contribute jointly in times of crisis, help stabilise the whole system, and support member states facing migration pressures. The solidarity mechanism will cover various situations, including the disembarkation of people following search and rescue actions, the pressure exerted by migration, crisis situations or other specific circumstances.

The paradigm shift in cooperation with third countries also aims to drive a common European return system, so that EU migration rules become more credible and to establish a common governance for migration, with better strategic planning to ensure the alignment of EU policies and national ones, as well as increased monitoring of migration management in the field, in order to strengthen mutual trust.

All the measures in the field of migration adopted by the European Union have a direct impact on guaranteeing the societal security in Romania, the fast way of implementation by the authorities being determined.

THE IMPACT OF THE COVID-19 PANDEMIC ON MIGRATION

The year 2020 is a benchmark in world history. It is the year in which all states face a significant global crisis, which began with a strong impact on health and which causes significant changes in the entire existence of human life.

The fight against the COVID-19 pandemic is not just a fight to defeat the virus, but a way to adapt to new world realities, to face a new global system that, in addition to the medical component, has also consequences for economic life, including in terms of migration.

Appearing at the end of 2019 in the Chinese city of Wuhan, the SARS-COV2 virus has spread quickly in all countries of the world, which led the World Health Organisation to establish the existence of a pandemic (Chappell, 2020), because of the very large number of countries where it has spread and the number of people infected, affecting the global health system.

One of the factors that favoured the increase in the number of people tested positive for COVID-19 was migration, given that many of the people who came from areas with a large number of cases had symptoms and there was a major risk of transmission in the family and communities of destination, considering that in Romania, according to the research carried out (GraphNets, 2020), the entry of the virus was facilitated by migration, the main source of epidemiological spread of the virus being Italy.

Therefore, gradual measures have been taken to try to limit the spread of the virus, depending on the number of cases of the disease.

The regulations imposed during the pandemic were similar in all European states, being considered absolutely necessary to protect public health in the international epidemiological context generated by the spread of SARS-COV2 virus, being exceptional and limited in time only for the period necessary to reduce the spread of the virus.

Regarding Romania, on 16 March 2020, Decree no. 195 (Sinteza, 2020) established a state of emergency in the country, which entailed, on the one hand, the restriction of several rights, including free movement and the adoption of measures with gradual applicability in the fields of public order, economy, health, labour market, justice and foreign affairs. At the same time, the same normative act required the closure of state borders, which obviously had direct consequences on migration and the isolation or quarantine of people from areas considered at risk, but also of those who had come into contact with them, for a period of 14 days.

Moreover, in the same context, in addition to the traffic restrictions imposed between European states, traffic restrictions were adopted between cities or even between neighbourhoods in the same city, leaving home being only allowed in exceptional situations, which obviously affected the mobility of citizens, including migration.

Failure to comply with the legal measures had as consequences both the payment of fines in high amounts and criminal sanctions, the facts constituting the crime of thwarting the fight against diseases provided by art. 352 of the Criminal Code.

Based on the Decree no. 195/2020, several military ordinances were adopted by the Ministry of Internal Affairs, which implemented specific measures, dosed according to the evolution of the number of cases tested positive for COVID-19.

Ever since the first military ordinance, on 17 March 2020, economic flights to and from countries with a large number of cases of people infected with the SARS-COV2 virus were suspended, the measure being necessary to limit the spread of the virus in Romania, which had a strong impact on migration.

In addition to the visible effect of affecting the free movement in European states to protect the general interest of public health, the measures adopted during the state of emergency and subsequently partially extended during the state of alert had a strong resonance on the worldwide economic sector (Forbes, 2020). Thus, the 2020 pandemic had as a side effect the suspension of the activity of certain sectors of activity during the state of emergency, which generated a large number of unemployed who did not come only from the directly affected state, migrants being included in this category. They worked mainly in the tourism sector (Lazăr, 2020), which suffered the strongest impact because of the traffic restrictions imposed by European states, the effects being felt in related activities, such as restaurants, in this industry being estimated (Albu) that 74% of activity will be closed, leading to 8.4 million jobs lost in Europe.

In this context, the European Union has established that funding needs to be allocated (Savu, 2020) to the member states for the protection of employees and employers affected by the pandemic, Romania receiving a grant of 4 billion euros in the form of a loan to maintain jobs until the full recovery of the economy (Văduva, 2020). As an effect of the pandemic on the labour market sector in relation to migration, there is also the development of telework activity, by digitising the activity. This applies to both domestic workers and migrants, in the context in which many multinational companies operating in fields compatible with online work have preferred since the beginning of the pandemic to no longer impose physical presence on employees at headquarters, but to encourage work at home, which leads to a substantial decrease (Marinescu&Căpuș, 2020) of the expenses made with the spaces in which the activity takes place, but also to an increase of the labour productivity.

Thus, workers have left for their home countries and continue to work online, which may represent a cost reduction for them and a total restructuring of the perception of migration in order to find a better job in another state, provided that it is found that the activity can be carried out through telework, with a remuneration at the standards of the employer's state of origin, but without being uprooted from the family of origin.

CONCLUSIONS

Migration is a reality of today's European society that will continue to exist as long as there are economic and financial gaps between EU member states and non-EU countries, its fluctuations being closely related to the evolution of state development.

The essential component of the European concept of space of freedom, equality and justice, the phenomenon of migration focuses mainly on the integration of migrants in the destination states and on guaranteeing their equality with the citizens of the respective state in order to respect non-discrimination, matrix principle of international human rights protection (Sudre, 2006, p. 202).

Although several European measures have been taken over time to combat illegal migration, it remains a challenge for the European space, which undermines the social security of the member states.

In order to adopt efficient policies in the field, it is necessary to take into account the practical problems in the field of migration identified in European countries, the success of implementing measures certainly depending on the specific areas to be applied, in the context of differences between states as well as within the same state.

Although migration brings a positive contribution to the destination states, mainly from the perspective of competitiveness on the labour market, the negative aspects in the context of the special social impact (Roman&Voicu, 2010, p. 64) produced on the family life of migrants should not be neglected.

In the context of the pandemic of 2020 generated by the COVID-19 virus, the concept of migration at European level has acquired new values, the movement of people between states being strongly affected, and the massive impact will be felt over several years (Chapagain).

The effective implementation of migration measures must imply a shared responsibility between the European Union and the member states, with the development of decisions capable of ensuring the maintenance of European societal security and of respecting the indivisible link between civil and political rights, on the one hand, and economic and social rights, on the other hand (Renucci, 2009, p. 10).

BIBLIOGRAPHY:

1. Beşteliu, R.M., Brumar, C. (2010). *Protecția internațională a drepturilor omului. Note de curs*. V^{th} edition. București: Editura Universul Juridic.
2. Corlățean, T. (2012). *Protecția europeană și internațională a drepturilor omului*. București: Editura Universul Juridic.
3. Dumitrescu, M., Căpuș, L. (2020). *Telemunca vs. munca la domiciliu în contextul COVID-19. Conformări și riscuri din perspectiva GDPR*, https://www.juridice.ro/679495/telemunca-vs-munca-la-domiciliu-in-contextul-covid-19-conformari-si-riscuri-din-perspectiva-gdpr.html, retrieved on 22 September 2020.
4. Lazăr, M. (2020). Digi 24, https://www.digi24.ro/stiri/economie/2020-anul-catastrofei-pentru-industria-turismului-este-de-departe-cea-mai-grava-criza-din-istorie-1307918?__grsc=cookieIsUndef0&__grts=53378886&__grua=ce4e9e986b0fbc713624d54b83c36283&__grrn=1, retrieved on 22 September 2020.
5. Muscalu, L.-M. (2015). *Discriminarea în relațiile de muncă*. București: Editura Hamangiu.
6. Peticilă, M. (2019). *În 2018, România a avut cea mai mare migrație din ultimii 9 ani: populația unui oraș cât Ploiești a plecat din țară*, https://www.edupedu.ro/in-2018-am-avut-cea-mai-mare-migrație-din-ultimii-9-ani-populatia-unui-oras-cat-ploiesti-a-plecat-din-tara/, retrieved on 1 September 2020.
7. Renucci, J.-F. (2009). *Tratat de drept european al drepturilor omului*. București: Editura Hamangiu.
8. Sudre, F. (2006). *Drept european și internațional al drepturilor omului*. București: Editura Polirom.
9. Ştefănescu, I.T. (2010). *Tratat teoretic și practic de drept al muncii*. București: Editura Universul Juridic.
10. Tofan, M., Petrișor, M.-B. (2013). *Dreptul muncii. Curs universitar*. București: Editura Hamangiu.
11. Văduva, D. (2020). *Pandemia COVID-19 a accelerat digitalizarea companiilor. Elemente cheie ale procesului de transformare*, https://blog.pwc.ro/2020/06/04/pandemia-covid-19-a-accelerat-digitalizarea-companiilor-elemente-cheie-ale-procesului-de-transformare/, retrieved on 13 September 2020.
12. Voicu, C. (2010). *Economie teoretică şi aplicată*. Vol. XVII, no. 7(548), http://www.store.ectap.ro/articole/484_ro.pdf, retrieved on 3 October 2020.
13. ESO (2020). *Communication on a New Pact on Migration and Asylum*, https://ec.europa.eu/commission/presscorner/detail/ro/qanda_20_1723, retrieved on 13 September 2020.
14. GraphNets(2020),https://unibuc.ro/un-grup-de-cercetatori-de-la-universitatea-din-bucuresti-a-modelat-statistic-primele-18-zile-de-circulatie-a-covid-19-in-România-2/?fbclid=IwAR2Im4CDeCgxUnqrzKA5bTg70-FIbQ-4aCx5JXpBDk7ASZ5x6jOCeCp_Bss, retrieved on 3 September 2020.

15. Institutul Național de Statistică (2019). *Tendințe sociale*, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Migration_and_migrant_population_statistics/ro, retrieved on 1 September 2020.
16. *EU Official Journal* (2020), https://eur-lex.europa.eu/resource.html?uri=cellar:85ff8b4f-ff13-11ea-b44f-01aa75ed71a1.0008.02/DOC_1&format=PDF and https://eur-lex.europa.eu/resource.html?uri=cellar:85ff8b4f-ff13-11ea-b44f-01aa75ed71a1.0008.02/DOC_2&format=PDF, retrieved on 29 September 2020.
17. Study: *Harta propagării infecției cu coronavirus în România* (2020), https://www.revistasinteza.ro/studiu-harta-propagarii-infectiei-cu-coronavirus-in-romania, retrieved on 12 September 2020.
18. *Tabăra de refugiați Moria în flăcări*, https://www.dw.com/ro/tab%C4%83ra-de-refugia%C8%9Bi-moria-%C3%AEn-fl%C4%83c%C4%83ri/a-54863219, retrieved on 29 September 2020.
19. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Migration_and_migrant_population_statistics/ro, retrieved on 1 September 2020.
20. https://www.edupedu.ro/in-2018-am-avut-cea-mai-mare-migrație-din-ultimii-9-ani-populatia-unui-oras-cat-ploiesti-a-plecat-din-tara/, retrieved on 1 September 2020.
21. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Migration_and_migrant_population_statistics/ro, retrieved on 1 September 2020.
22. http://legislatie.just.ro/Public/DetaliiDocument/229857, retrieved on 1 September 2020.
23. https://www.dw.com/ro/opinie-nu-suntem-%C3%AEn-stare-de-nimic-la-moria/a-54905440, retrieved on 21 September 2020.
24. https://www.dw.com/ro/tab%C4%83ra-de-refugia%C8%9Bi-moria-%C3%AEn-fl%C4%83c%C4%83ri/a-54863219, retrieved on 11 September 2020.
25. https://eur-lex.europa.eu/resource.html?uri=cellar:85ff8b4f-ff13-11ea-b44f-01aa75ed71a1.0008.02/DOC_1&format=PDF, retrieved on 11 September 2020.
26. https://ec.europa.eu/commission/presscorner/detail/ro/qanda_20_1723, retrieved on 1 September 2020.
27. https://www.npr.org/sections/goatsandsoda/2020/03/11/814474930/coronavirus-covid-19-is-now-officially-a-pandemic-who-says?t=1601362103707, retrieved on 11 September 2020.
28. https://unibuc.ro/un-grup-de-cercetatori-de-la-universitatea-din-bucuresti-a-modelat-statistic-primele-18-zile-de-circulatie-a-covid-19-in-România-2/?fbclid=IwAR2Im4CDeCgxUnqrzKA5bTg70-FIbQ-4aCx5JXpBDk7ASZ5x6jOCeCp_Bss, retrieved on 12 September 2020.
29. https://www.revistasinteza.ro/studiu-harta-propagarii-infectiei-cu-coronavirus-in-romania, retrieved on 12 September 2020.
30. http://legislatie.just.ro/Public/DetaliiDocumentAfis/223831, retrieved on 1 September 2020.

31. https://www.forbes.ro/efectele-coronavirusului-asupra-economiei-si-masurile-luate-de-statele-europene-pentru-ajuta-firmele-afectate-155207, retrieved on 1 September 2020.
32. https://www.digi24.ro/stiri/economie/2020-anul-catastrofei-pentru-industria-turismului-este-de-departe-cea-mai-grava-criza-din-istorie-1307918?__grsc=cookieIsUndef0&__grts=53378886&__grua=ce4e9e986b0fbc713624d54b83c36283&__grrn=1, retrieved on 1 September 2020.
33. https://academiaromana.ro/SARS-CoV-2/doc/d08-Impactul_macroeconomic_al_COVID-19.pdf, retrieved on 1 September 2020.
34. https://blog.pwc.ro/2020/06/04/pandemia-covid-19-a-accelerat-digitalizarea-companiilor-elemente-cheie-ale-procesului-de-transformare, retrieved on 1 September 2020.
35. https://www.juridice.ro/679495/telemunca-vs-munca-la-domiciliu-in-contextul-covid-19-conformari-si-riscuri-din-perspectiva-gdpr.html, retrieved on 1 September 2020.
36. http://www.store.ectap.ro/articole/484_ro, retrieved on 1 September 2020.
37. https://www.orange.ro/info/news/mediafax/article/2972067, retrieved on 2 October 2020.

IMPORTANT STAGES IN THE DEVELOPMENT OF THE EU CAPACITY TO PERFORM AUTONOMOUS OPERATIONAL COMMITMENTS. CASE STUDY – OPERATION ARTEMIS

Dragoș ILINCA

Institute for Political Studies of Defence and Military History

In 2003, the EU decided to develop the operational tempo by launching its very first military operation in the Democratic Republic of Congo. Known as "Operation Artemis", this represented an essential stage within the process of developing the EU autonomous profile in crisis management.

By using the case study of Artemis Operation as a research method, I intended to highlight the development of the main parameters of the future EU operational design. Within this approach, I also followed the process of setting-up the conceptual framework related to rapid reaction capabilities, especially Battle Groups. In this respect, Artemis had an essential role in adapting European cooperation to the challenges of planning and executing tasks in a demanding operational environment.

Keywords: European defence; EU-NATO; Petersberg tasks; Battle Groups; European Security and Defence Policy;

INTRODUCTORY CONSIDERATIONS ON THE DEVELOPMENT OF THE EU SECURITY AND DEFENCE DIMENSION

Since its initial stages, European defence cooperation was centred on the development of the operational capacity to be able to act across the full range of Petersberg tasks. In this respect, the legal framework adopted by the European Council in December 1999 indicated the options that the EU could employ in planning and deploying its operational commitments. The approach was two-fold, including the option of using NATO's capabilities and conducting autonomous operations, based on member states contributions. Stemming from the EU-NATO cooperation framework (underpinned by the "Berlin+" Agreements), the first option was used in the Western Balkans, where EU gradually assumed the main responsibilities for security evolutions in this region.

At the beginning of June 2003, European Union adopted the operational plan and the decision to launch its very first crisis management operation (Official Journal of European Union 2003, L147, 14.06.2003, p. 42), which would be deployed several days later, in the Democratic Republic of Congo. Latter known as *"Operation Artemis"*, it represented a new feature in the overall international context of that period. At the same time, it was integrated within a complex security environment, having in mind both the development of the EU role in defence and security and particular evolutions in Africa. Thus, the decision to launch such an operational undertaking must be seen from several perspectives.

First, the decision was taken in an initial, but decisive, sequence of the European cooperation development process. The conceptual inception of this approach could be depicted easily in the framework of the Franco-British Declaration adopted at St. Malo, in December 1998. It was highlighted that the EU had to develop the required capacity to be able to autonomously launch and manage crisis management operations (Rutten, 2001, pp. 8-10). This objective was undertaken, one year later, in the decisions adopted by the Helsinki European Council (9-10 December 1999) regarding the development of the first Headline Goal, under the newly created European Security and Defence Policy (ESDP). It aimed at the creation, by 2003, of a rapid reaction force, comprising 50-60,000 military personnel, deployable in 60 days and sustainable for 1 year (Rutten, pp. 82-92).

Within this framework, launching an autonomous commitment was meant to enhance the identity of the EU's role and contribution. At the same time, it must be analysed as a direct consequence of the political ambitions associated with this process, which emulated in the first half of 2003 on the development of European cooperation project in security and defence. This approach was reflected in two other decisions adopted in that period, namely, launching, on 1 January 2003, the civilian police mission in Bosnia-Herzegovina (EUPM BiH) and the first military EU operation, Concordia, deployed in Macedonia. The last one was designed as a follow-on operation after the NATO mission *"Allied Harmony"*, thus being a direct legal reflection of the agreement regarding operational cooperation between EU and NATO, signed in December 2002. Much better known as the *"Berlin+ Agreements"*, these were designed to establish the procedural framework through which the EU would be able to use NATO's planning and C2 capabilities for conducting its crisis management operations. At the same time, defining this cooperation framework supported the process of assuming a more prominent role by the EU in the management of security evolutions in Western Balkans.

As regards the overall parameters of the European project, the operational components were meant to develop based on two typologies, one related to the operations with recourse to NATO support and the other focused on autonomous operations, generated through member states contributions. This approach was agreed in the framework of EU-NATO negotiations being formalised in a cooperation framework (Rutten, pp. 172-173), adopted by both organisations through the European Council in Nice (12 December 2000) and, a few days later, by NATO Foreign Ministerial Meeting which took place in Brussels, on 14-15 December 2000.

Within this framework, Artemis was an initial formula for testing the autonomous capacity that the EU could undertake in developing an operational commitment. Obviously, this decision should be seen from the perspective of the European capabilities development process. As it was mentioned, the European cooperation reached a certain maturity, especially in terms of fulfilling the Helsinki Headline Goal. In this sense, Laeken European Council (14-15 December 2001) launched the European Capabilities Action Plan (ECAP), which was meant to improve the capability gaps identified in the HLG 2003 implementation process. The final report made by the experts involved proposed several solutions to mitigate the shortfall. From this perspective, the EU defence ministers adopted, during the Capabilities Commitment Conference (Brussels, 19 May 2003), a Declaration, stating, *"EU will be able to carry out the full range of Petersberg Tasks"* (Declaration of the Capabilities Commitment Conference, 2003).

LOCAL CONDITIONS OF AN UNSTABLE SECURITY ENVIRONMENT IN THE DEMOCRATIC REPUBLIC OF CONGO

In addition to the aspects related to the ESDP development and EU-NATO cooperation, the decision to launch Artemis Operation was also related to the security evolutions in RD Congo. The main aspect was the overall spreading of the conflict in this area generated by a continuous interlinkage between ethnic clashes and competition for natural resources in Ithuri province. Within this framework, the massive degradation of the security situation involved most of the countries in the region as well as the growing number of the armed groups and militias. The conflict developed with different level of intensity on different regions in RD Congo but since 1998, it concentrated in the province of Ithuri. Between 1999-2003, the number of victims of the civilian population increased significantly, reaching, according to Human Rights Watch, 50,000 people (Human Rights Watch, 2003).

International efforts regarding the normalisation of local security generate the conditions for signing of an Agreement of ceasefire (Lusaka, 10 July 1999) between all countries from the area (Angola, RD Congo, Namibia, Uganda, Rwanda and Zimbabwe). The main provisions stipulated the termination of fighting and violence on all Congolese territory. Moreover, it called for a peacekeeping mission, which will monitor the implementation process, while over sighting the disarmament actions related to militias and rebel groups. Based on this request, the UN Mission *(Mission de l'Organization des Nation Unissien en République Démocratique du Congo – MONUC)* will be deployed at the end of the year, based on Security Council Resolution 1279/30 November 1999. The initial mandate included tasks related to monitoring the ceasefire implementation and the withdrawal of the regular forces of neighbour countries from the Congolese territory. Afterwards, by adopting Resolution 1291/24 February 2000, the Security Council authorised the increase of MONUC strength to 5,537 personnel, including 500 monitors.

Under these favourable auspices, in 2002, there were several other initiatives related to the withdrawal of foreign armed forces. Supported by the mediation of South Africa and Angola, bilateral agreements were signed between RD Congo and Rwanda (30 July 2002), followed by a similar one with Uganda (6 September 2002). Unfortunately, the window of opportunity closed very fast because of the armed groups resumed the attacks against the civilian population. In the wake of the decision of withdrawing foreign forces from RD Congo, the rebel groups engage in forceful actions to get more control. The capital of Ithuri province, Bunia, became the centre of extreme violence (Stale&Gurlag, 2004, p. 511), which forced the local population to find shelters in the small areas protected by MONUC presence, which did not manage to increase (Taylor&Williams, 2004, p. 208) significantly its presence. In this context, even the UN offices in Bunia are targeted by the armed group's attacks, while more than 50.000 people are trying to find their salvation in neighbouring countries.

On 15 May 2003, UN Secretary-General, Kofi Annan, made an appeal for international involvement in Bunia as a temporary measure until new MONUC contingents would be ready for deployment. Following its undertaking, several countries, like France, Canada, UK, South Africa and Pakistan express firm commitments. Simultaneously, Kofi Anan sent to EU an official request to explore the possibilities to contribute under ESDP. The High Representative, Javier Solana, presented the request to the EU defence ministers during a ministerial meeting in Brussels, on 19 May 2003. The option of a concrete contribution in support of the stabilization process in Ithuri/Bunia gathered the member states support. Therefore, the defence ministers adopted the decision (Kirk&Beatty, 2003) to initiate an analysis to review the options at hand.

It must be underlined the fact the discussions in the EU were enabled by the firm option made by France to assume an operational role within this framework. In the wake of the Anglo-French summit of Le Touquet, on 4 February 2003, it was expressed the commitment of those countries towards a more robust profile of EU in the crisis management field. From this perspective, the option of developing concrete contributions in support of the security situation in Africa, including through an autonomous ESDP operation (Missiroli, 2003, pp. 36-40) was advanced as the main option for the next period. Based on that, on 28 May 2003, France announced its availability to assume a framework-nation role for a future EU operational commitment in Bunia.

MAKING THE EU POLITICAL DECISION IN THE DEMOCRATIC REPUBLIC OF CONGO OPERATIONAL

Following the political consensus achieved in EU, in 30 May 2003, the Security Council adopted Resolution 1484 regarding the mandate of an Interim Multinational Emergency Force (IEMF), which was planned to intervene in Bunia. The main objective was to develop the legal framework for a multinational deployment in the hot spots of Bunia as a transitory measure, until 1 September 2003, on the assumption that the MONUC presence will be increased significantly by the middle of August. From this perspective, IEMF actions would be carefully coordinated with MONUC as well as with its forwarded elements in Bunia. It was envisaged as a major priority ensuring the full control on the local airport, to allow the free movement of transportation for MONUC and to implement effective protection measures for the refugees who sheltered in this area. Moreover, the IEMF mandate included tasks related to the protection of refugee camps, international personnel, the safety of the civilian population and NGOs. As can be seen, IEMF mandate corresponded to a conflict zone with a high degree of unpredictability and requiring high-intensity operations. From this perspective, the mandate given to the international force was a robust one, being drafted on the base of Article VII of the UN Charter.

The EU answer to these evolutions has materialised in the adoption of Joint Action 423/5 June 2003, which structured the main parameters of the EU mission in DR Congo. Having in mind the total novelty for EU of this kind of commitment, the generation process was centred on capitalising France commitment to provide the main line of effort. In this sense, the planning process was conducted under the Framework Nation Concept for EU autonomous operation, adopted on 24 July 2002 (EU Framework Nation Concept, 2002).

As regards C2 arrangements, the main responsibilities were fulfilled by France, which made available the Operational Headquarters, through *Centre de planification et de conduit des Operations* in Paris under the command of major general Bruno Neveaux. Other member states contributed with staff personnel to this structure for the entire duration of the operation. At the same time, based on the Framework Nation Concept, France filled the force commander position, also, through brigadier general Jean-Paul Thonier. Within this framework, the EU Council, approved, on 8 June 2003, OPLAN and Rules of Engagement paving the way for the adoption of the decision to launch the operation (10 June 2003).

The political coordination and strategic guidance were provided through the Political and Security Committee (PSC). The main responsibilities for deciding of the objectives and engagement period rest with EU Council, assisted by the High Representative who was also responsible for ensuring the main interface with the UN for the entire duration of the operation. From the military perspective, the Military Committee performed the main duties in monitoring the implementation process and reporting periodically on the evolutions.

In the field, the Artemis presence benefited extensively from French presence. Within the overall context of diplomatic dialogue between Kofi Annan and French president, Jacques Chirac, on 20 May 2003, French army deployed a reconnaissance team. The results of this mission were used in the planning process and to the preparation of the deployment of the initial elements on 6 June 2003. The deployment process was conducted, extensively, by using the infrastructure elements maintained with French support on the airfields in Chad (N'Djamena) and Uganda (Entebbe). The main problem that had to be managed by the European planners was to ensure enough strategic transport capabilities for the entire deployment requirements. The complexity of this aspect was increased by a few factors including distance between embarkation point and operational area (almost 6.500 km); technical incompatibility between local airports infrastructure and transportation capabilities and hostile conditions in the local security environment. All of these challenges were overcome with significant efforts made by the French and British engineering units in maintaining the landing strips operational. This was the most complex issue because of a major incompatibility (Firenze, 2003, p. 42) between landing strips quality and planes used for deployments (C-130 Hercules, C-160 Transall, DC-8, Airbus 310). At the same time, the national contributions in the field of air transportation increased significantly through capabilities made available by Germany, Belgium, the United Kingdom and some of the third countries. The role made by these countries was essential which is the case for Canadian and Brazilian airplanes operating from Entebbe since the operational conditions did not allow to operate (Smith, 2017, p. 117) direct flights from Europe towards Bunia. Therefore, a significant number of tactical flights were organised between Entebbe and Bunia, on a smaller distance (300 Km). Ensuring the required flight hours determined, also, to rent additional flights of Ukrainian Antonov AN-124 (approximately 40 hours).

IMPLEMENTING THE MANDATE OF EU MISSION ARTEMIS

Force HQ was established in Entebbe, together with the logistic hub for the entire operation (Joint Support Base) while the opening of a forwarded element in Bunia. The fighting nucleus of the EU commitment (Multinational Combined Arms Tactical Group) was structured along with the profile of and enhanced infantry battalion with high mobility and autonomous logistic capability. The main line of effort was provided by France (almost 90% from the entire force) out of a maximum 2,100 military strength. French contribution was augmented with participation in the field of the Swedish Special Forces. In addition to that, there were various contributions made available by several member states, especially with staff personnel in the HQ in Paris (Austria, Greece, Hungary, Ireland, Italy, Netherlands, Spain, Portugal). For sustaining the operation on the ground, UK, Belgium and Germany deployed logistic and medical units in Bunia and Uganda.

The deployment finished by 6 July 2003. The main component of forces moved in Bunia consisted of French and Swedish units, around 1,300 troops, including logistic support. The MEDEVAC capabilities were provided by Germany on the Entebbe airport and by South Africa with transport helicopters. The force protection component was ensured also by France including armoured and anti-tank vehicle, ERC 90 – Sagaie. Without immediate applicability, there were provided with some air support and reconnaissance capabilities through French fighters (Mirage 2000D and F1CT/CR) operating from the airports in Chad and Uganda.

The entry of forces in the operational area was made since 6 June 2003, the main actions performed by French contingent focusing, initially, on securing the airport and immediate neighbourhood. Gradually, pending on the deployment pace (on 13 June the strength of EU contingent reached 400), the control was expanded on the main junctions road in Bunia.

In executing these tasks, there were some attacks from rebel groups which were rejected successfully by EU contingents. Simultaneously, the offensive capacity of armed groups was diminished significantly by blocking the supply routes used by them. One week later, the firm pressure made by Artemis paid off. Almost 2.500 rebels left, by the end of 25th of June, the city of Bunia. Based on that, the EU mission took control over the entire city allowing the distribution of humanitarian assistance and the return of more than 50,000 refugees in the province capital.

Furthermore, the actions undertaken by Artemis Operation continued in July 2003, contributing to the full demilitarization of Bunia and eradication of the armed group's presence within the adjacent perimeter of Ithuri capital. From this perspective, on 8 July 2003, Bunia was declared demilitarised zone, paving the way for adopting, on 28 July 2003, of the Resolution 1493, which increased the MONUC presence at 10,800 troops.

According to the initial planning, in the middle of August 2003, was initiated the transition period (15 August – 1 September) in which the transfer process was conducted towards MONUC, both in Bunia and immediate neighbourhood. This process involved the first UN contingent arrived in Ithuri, including a brigade of Bangladesh troops (almost 4.800 troops). The last stages of the handing over process were conducted between 1 and 7 of September 2003, the last Artemis elements being gradually withdrawal until 25 September 2003 when Entebbe and Bunia bases were closed (United Nations Peacekeeping Best Practice Unit Report, 2004).

CONCLUSIONS

There is no doubt that Artemis Operation is one of the essential moments in developing EU capacity to undertake autonomous operations both in terms of generation process as well as effectiveness in implementing mandate objectives. The analyses of the period indicate the success of EU operation being a model on how a demanding operational commitment could be generated in a complex and volatile security environment. In this regard, the actions performed by Artemis had a positive impact on stabilising local security situation. This can be depicted in the return of refugees contributing to the overall consolidation of the negotiation framework for improving the security situation in DR Congo.

At the same time, the importance of this operation should be seen from the perspective of European cooperation in security and defence. Planning, generation and the practical action in the field tested the EU institutional capacity to manage such a commitment towards a new Level of Ambition in ESDP and CSDP developments. On a similar extent, through Artemis, the EU becomes an international reliable partner in the field of crisis management. From this perspective, it represented the starting point in developing EU-UN Partnership being, also, the first practical interaction between those two organisations in the operational environment.

On similar coordinates, the EU commitment initiated a more enduring commitment in DR Congo, which will be developed substantially in the coming period through successive operational commitments in various domains associated with the security sector reform.

From a more practical perspective, Artemis represented the essential component for completing the conceptual inventory of EU in the field of crisis management. It paved the way for the Battle Groups concept, which represented the backbone of Headline Goal 2010, adopted by the European Council in June 2004. The structural features used in generating the contingents deployed in DR Congo, were integrated, from now, on for establishing different formats of EU Battle Groups. Thus, criteria such as the speed of decision-making process, pace of deployment, internal force structure, the model of ensuring the logistic support were all incorporated as such in the parameters of EUBG.

We should take into account, also, the particular context of European cooperation evolutions in which Artemis was launched. The undertaking of this commitment overlapped with an important validation stage of the signs of progress achieved in implementing EU objectives in security and defence, adopted by the European Council in Helsinki. From this perspective, Artemis could be seen as generating additional opportunities for testing the European solidarity in assuming a more robust profile of the EU in crisis management.

Although there were persisting capabilities shortfalls in the implementation of Helsinki Headline Goal, especially on C2 and airlift, these were overcome by using international cooperation formulas which augmented the French contribution. From this perspective, Artemis experience could be used as a model, both for planning and generation process as well as on the opportunities to involve third countries in CSDP context.

BIBLIOGRAPHY:

1. Firenze, N. (2003). *EU Forces Seeks New Mission After Congo*. Defence News.
2. Kirk, L., Beatty, A. (2003). *European Forces for Congo Peace Mission*, https://euobserver.com/news/11289/, retrieved on 16 August 2020.

3. Missiroli, A. (2003). *Declaration Strengthening European Cooperation in Security and Defence*. French-British Summit, Le Touquet. In Chaillot Papers, nr. 67, From Copenhagen to Brussels: European Defence Core Documents, vol. IV, EU Security Studies Institute, Paris, 2003.
4. Rutten, M. (2001). *From St. Malo to Nice: European Defence: Core Documents*. Chaillot Paper 47, Paris: ISS Western European Union.
5. Smith, M. (2017). *Europe's Common Security and Defence Policy*. Cambridge: Cambridge University Press.
6. Stale, U., Gurlag, C. (2004). *Operation Artemis: The Shape of Things to Come?*. International Peacekeeping, vol. 11, nr. 3.
7. Taylor, I., Williams, P. (2004). *Africa in International Politics: External Involvement on the Continent*, Routledge.
8. *EU Framework Nation Concept*, https://data.consilium.europa.eu/doc/document/ST-11278-2002-REV-1/en/pdfa/ retrieved on 16 August 2020.
9. *Military Capabilities Commitment Declaration* (2003), https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/misc/Military%20capabilities%20-%20EN.doc.html/, retrieved on 12 August 2020.
10. Human Rights Watch, *Ithuri: "Covered in Blood". Ethnically Targeted Violence in Northeastern DR Congo*. Vol. 15, nr. 11, New York.
11. Official Journal of European Union 2003, L147, 14.06.2003, https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:32003D0432&from=EN, retrieved on 5 August 2020.
12. United Nations Peacekeeping Best Practice Unit Report – 2004.

REALITIES AND PERSPECTIVES OF EU-NATO COOPERATION IN SECURITY AND DEFENCE

Major Romeo BUHAI, PhD Student

"Carol I" National Defence University, Bucharest

The scale of geopolitical changes over the past decade has led major regional and global actors to re-evaluate their options, identify new ways of responding to threats and risks in the international security environment, by adapting theirs security policies and strategies, on the one hand, and, on the other hand, by participating into new partnerships or other forms of institutional and military cooperation, or through the development of existing ones.

NATO-EU security and defence cooperation is part of this trend of reconfiguring the current security environment, trying to identify the best solutions that respond effectively to current and future threats, while maintaining a balance on the role of the two major organisations in achieving this goal.

The article broadly outlines the progress made by the European Union in extrapolating its role, from that centred on the economic field to that of security and defence, in the organisation's determination to become a leading security actor at regional and global level.

Keywords: EU; NATO; Permanent Structured Cooperation; military capabilities; military mobility; cybersecurity;

INTRODUCTION

Since its emergence, the concept of *security* has aroused an increased interest in its study, through the determining relationships between it and the environment in which it manifests its effects, through the different intertwining of the concept with the other twists of the environment trying to delineate and understand most of the processes and phenomena that define human society. Becoming one of the most important concepts of the science of international relations, whether it relates to an individual, a state or even the international environment, security has been, is and will continue to be a concern for researchers in the field in an attempt to discover its roots, to highlight its interdependencies and to understand its metamorphoses. All of these are necessary in order to predict its developments and identify the best solutions to preserve the safety, stability and even the existence of human society.

The end of the 20th century and the beginning of the 21st century led to the writing of a new chapter in the evolution of the international security environment, the fall of the main bastions of communism, the evolution towards multipolarity, the growing trend of expanding globalisation, as well as the emergence of new types of risks, threats and extrapolation of existing ones, requiring a rethink of the approach to the security environment, and implicitly adaptations to the security policies and strategies of prominent actors, both regionally and globally, in an attempt to create the best conditions and solutions to maintaining/expanding the spheres of influence and ensuring peace and prosperity worldwide.

Current threats rapide propagation, their increased capacity to transform and adapt to the environments in which they operate, and their effects on the interests of major security actors as a cause of theitr concrete manifestations have also led the actors to understand that no matter how powerful they are, they will not be able to face the challenges alone, thus being necessary to make a unitary front and develop forms of international cooperation.

In this respect, the cooperation of the European Union (EU)-North Atlantic Treaty Organisation (NATO) in the field of security and defence is one of the eloquent examples, the strategic partnership between the two international actors being reconfirmed and raised to ever-higher levels.

EU-NATO SECURITY AND DEFENCE COOPERATION COORDINATES

Over time, the concept of security has multiplied its meanings in close correlation with the characteristics of the international environment. If the Explanatory Dictionary of the Romanian Language (1998) defines security as *"that state of affairs which protects from any external and internal danger a collective or any state, following specific measures that are adopted and which ensure the existence, independence, sovereignty, territorial integrity of the state and respect for its fundamental interests"*, the renowned theorist Barry Buzan is one of those who have contributed decisively to the extension of the scope of the meanings of the concept. In this respect, security is addressed multisectorally, along with the military sector including the economic, social, political and environmental sectors, as well as their relations. Building on this approach, today, ensuring security is more than ever dependent on the mastery of states to direct their efforts in cooperation and the conclusion of alliances and partnerships, at both regional and global level.

If NATO has been a political-military organisation focused mainly on ensuring and guaranteeing security since its inception, we cannot say the same about the EU, an organisation that at the time of its establishment had a political and purely economic profile. It therefore becomes interesting to follow how the two world-class organisations have managed to conclude and develop this partnership to the very end, as defined by the London Summit Declaration of December 2019, the document highlighting, among other things, unprecedented progress.

A key question we will try to answer is: *How did the European Union, from a political and economic integration organisation, come to expand its interests in the sphere of security and defence?* The idea of a European security and defence identity was originally formulated in the framework of the Single European Act of 1986 and was later developed within the framework of the Western European Union (WEU) Platform on European security interests and the 1992 Maastricht Treaty. However, we consider that the starting point in the development of the concept of security and defence at the EU level is considered to be the Cologne Summit of June 1999, Annex III of the European Council Declaration on strengthening the European Security and Defence Policy (ESDP), stating that *"the European Union will play its full role on the international stage. To this end, we intend to provide the European Union with the means and capabilities necessary to assume the specific responsibilities of a European Security and Defence Policy"* (European Council, 1999).

Within the framework of cooperation, it is NATO that has the full range of military capabilities necessary to ensure and guarantee security, and the EU has a complex range of diplomatic, economic and social institutions, thus complementing NATO's institutional framework. In this regard, between 2000 and 2002, both the EU and NATO adopted a series of measures governing the participation of European NATO member states as well as other states in EU-led activities/missions for crisis management, EU-NATO cooperation in crisis prevention and management, and the provision of NATO's collective capabilities to the EU. The confirmation of the measures taken at NATO and EU level was provided on 16 December 2002, by issuing the EU-NATO Declaration on ESDP and signing the *"Berlin+"* agreement. The declaration stipulates the principles on the basis of which the partnership will be conducted, as follows: *"mutual consultations, dialogue, cooperation and transparency; equality and respect for decision-making autonomy and the interests of NATO and the EU; respect for the interests of the members of the two organisations; respect for the principles of the UN Charter and the development of the necessary military capabilities common to the two organisations in a coherent, transparent manner and on the principle of mutual consolidation"* (EU-NATO Declaration on ESDP, 2002).

An important step taken by the EU ocurred in December 2003 when the European Security Strategy was adopted. Thus, by carrying out a joint assessment of existing threats to the EU, principles, directions of action and strategic objectives for promoting the organisation's security interests, such as: the global threat approach, building and strengthening security in the EU's neighbourhood, and developing an international order based on effective multilateralism, were included for the first time. At the same time, the importance of partnership with NATO in the document is also stressed by stating the following: *"for Europe, the transatlantic partnership remains an irreplaceable foundation based on shared history and responsibilities. The EU and NATO must deepen their strategic partnership for better cooperation in crisis management"* (European Security Strategy, 2003).

The EU continued its evolution in the field of security and defence by setting up, on 12 July 2004, the European Defence Agency (EDA), initially its mission being *"to support EU Member States in their efforts to improve European defence capabilities in the field of crisis management and to support the European Security and Defence Policy in its current form and its future updates"* (European Defence Agency). The Agency's mission has now evolved, its current effort being focused on achieving three key tasks: supporting the development of defence capabilities and military cooperation between EU Member States; boosting research, development for defence and strengthening the European defence industry; and acting as military interface in the implementation of EU policies.

After a five-year period of continuously efforts in the field of security and defence in conjunction with the international security environment's developments, the Treaty of Lisbon enters into force on 1 December 2009, the ESDP being improved and renamed as the Common Security and Defence Policy (CSDP). Seeking to address identified dysfunctions within the various forms of cooperation between Member States, *"the purpose of the Treaty is to create more efficiency and coherence in action"* (Duțu, Bogzeanu, 2011, p. 42), thereby increasing the EU's visibility and role in the international environment. CSDP brings new elements, particularly in the field of the development of civil instruments and mechanisms for managing international crises and conflicts. In this respect, the share between civil and military operations carried out after the entry into force of the Treaty is relevant.

As a novelty, the Treaty provides for the establishment of institutions and functions aimed at optimising the flow of decision-making, the most relevant for security and defence being: the function of High Representative for Foreign Affairs and Security Policy (HRFASP) and the institution of the European External Action Service (EEAS). The Convention also establishes the legal framework for the operation of the European Defence Agency and extends the variety of EU missions, with the following added to their range: *"joint disarmament actions, humanitarian and evacuation missions, military advice and assistance missions, conflict prevention and peacekeeping missions, armed forces crisis management missions, including peace-building missions and post-conflict stabilisation operations"* (Eur-Lex).

The introduction, within the framework of Article 42 of the Treaty, of the obligation for all EU members to provide the necessary assistance and support to any state within the organisation in the event of any armed aggression is of great importance to the field of security and defence. If at NATO level the responsibility of collective defence falls under the responsibility of the organisation, at EU level this obligation is the responsibility of each member state and not of the organisation itself. Viewed from this direction, the regulation of mutual assistance is intended to increase cohesion between member states. Cooperation with NATO continues to be a fundamental coordinate of the development and security of the EU, as set out in the text of the article: *"commitments and cooperation in this area are in line with the commitments made under the North Atlantic Treaty Organisation, which remains for the Member States of this organisation the foundation of their collective defence and the framework for its implementation"* (Ibid.).

The European Council in Brussels in December 2013 is the framework for the first debate on defence since the signing of the Treaty of Lisbon. Taking into account the analysis presented prior to the deployment of the Board by the Secretary-General of NATO, the priority actions to be carried out in this area are identified. In this respect, the effort is oriented in three directions of action: increasing the effectiveness, visibility and impact of the CSDP; supporting capability development; strengthening and developing the European defence industry. It is underlined once again, the EU's openness to cooperate with its regional and transatlantic partners, and the need to develop these partnerships in the spirit of strengthening relations and achieving complementarity.

The expansion of the EU's security and defence interests has also required changes in the organisation's security strategy and policies. Thus, the crises facing the EU, the need to respond to threats from either the neighbourhood of the Union's borders or existing globally, led to the development and issuance, on 28 June 2016, of the European Union's Global Strategy for Foreign and Security Policy. According to the speech of the EU's High Representative for Foreign Affairs and Security Policy, Federica Mogherini, strategic thinking, a common vision and a unified mode of action at EU level are needed to limit the manifestation of threats both inside and outside the organisation. In this respect, the structure of the Global Strategy is focused on five main priorities: the security of the Union; the resilience of states and societies in the East and South of the Union; an integrated approach to conflict; regional orders based on cooperation; and global governance for the 21st century.

Through this strategy, the EU aims to identify the best ways and responses to effectively address and resolve the crises it faces, whether internal or external. Moreover, another aim is to create means and mechanisms, strengthen member states' military and civilian capabilities in order to achieve interoperability both within the EU in order to be able to act independently if needed and with NATO in order to ensure complementarity in the conduct of joint missions. In order to achieve this level of ambition, while enabling the protection of the Union and its citizens, the effort must be geared towards setting priorities in the area of capability development, strengthening cooperation and increasing cohesion between member states, adapting structures, instruments and mechanisms, and not least strengthening and developing partnerships. While there have been critical voices in relation to this bold EU strategy, saying that it could lead to competition between the two major actors in the future, I believe that the provisions contained therein reinforce the idea that NATO remains central to EU security and defence. Thus, the Security and Defence section contains an eloquent paragraph to that effect, stating the following: *"as regards collective defence, NATO remains the main framework for its achievement for most Member States. At the same time, EU-NATO cooperation relations must not prejudice the security and defence policies of non-NATO EU members. Consequently, the EU will deepen cooperation with NATO* *in complementarity, synergy and full respect for the institutional framework and decision-making autonomy of both actors"* (EEAS, p. 20).

The signing of the NATO-EU Joint Declaration at the Warsaw Summit on 8-9 July 2016 takes the strategic partnership between the two organisations to another level. Recalling emerging challenges in the international security environment, the statement reiterates the need to develop partnership and increase the level of ambition. Thus, this can be achieved by: boosting actions and measures taken to counter hybrid threats; adapting structures and developing operational cooperation in areas such as the maritime environment, migration, security and cyber defence; the development of coherent, interoperable defence capabilities and participation in joint projects in this regard; increasing transatlantic cooperation in research, defence development and defence industry; improving coordination and increasing cohesion and interoperability between NATO and EU structures by participating in joint exercises, not least by building security and defence capacity and encouraging the resilience of its Eastern and Southern neighbours.

The implementation of the measures established under the Partnership is carried out through the European Defence Action Plan, presented by the European Commission in November 2016. The document identifies the common capacities needed to be developed, ways of efficient spending of funds, and supports the development of the European defence industry. Addressing different but complementary needs that arise during capacity development, the effort is focused around three basic pillars: the establishment of a European Defence Fund (EDF), the encouragement of investment in defence supply chains, and the strengthening of the Single Defence Market.

Subsequently, at the beginning of December 2016, the Implementation Plan on Security and Defence under the EU Global Strategy is approved. The document sets out the level of ambition and the following directions for the development of EU security and defence policy: effective management of external conflicts and crises, strengthening the capacities of partners and ensuring the protection of the Union and its citizens. In order to achieve the set objectives, there are identified the following steps needed to be taken: the creation of a Permanent Structured Cooperation (PESCO), the creation of a Military Planning and Conduct Capability (MPCC), the establishment of a European Defence Fund (EDF), the conduct of a Coordinated Annual Review on Defence (CARD) and the development of the EU Rapid Response Assets. They are also approved in parallel, by both the EU Council and the North Atlantic Council, 42 proposals on the implementation of the EU-NATO Joint Declaration, in the following areas: countering hybrid threats, operational

cooperation including maritime, security and cyber defence, defence capabilities, defence and research industry, exercises and development of security and defence capabilities.

The European Council of 15 December 2016 is part of the actions and measures taken during the year in the field of security and defence, reiterating once again the importance and need to strengthen this area. Thus, the significant level the EU-NATO cooperation has reached is highlighted, which is also highlighted in the joint statements of Presidents Donald Tusk, Jean Claude-Juncker and NATO Secretary General Jens Stoltenberg: *"working more closely than ever, the EU and NATO are of significant importance in ensuring the security and well-being of many millions of people"* (Taking EU-NATO Cooperation).

The year 2017 is one of measuring the full progress in implementing decisions taken in the field of security and defence, while at the same time making decisions establishing new capabilities. Thus, in the Council conclusions on security and defence in the context of the EU Global Strategy of 18 May 2017, progress in the following areas is highlighted: crisis management; improving cooperation in the field of CSDP with partner countries; capacity-building for security and defence; development of civilian crisis management capabilities and development of defence cooperation.

The need to establish a European structure for the management of military missions in the field of security and defence is also identified. To this end, on 8 June, the Council approved the establishment of the Military Planning and Conduct Capability (MPCC) within the EU General Staff. On the role of this capability, EU High Representative Federica Mogherini stated: *"the establishment of the MPCC is a very important operational decision for strengthening European defence. This will help to increase the effectiveness of non-executive European missions and improve the training of soldiers in partner countries, to guarantee peace and security. This is important not only for our partners, but also for the security of the European Union"* (EU Cooperation, 2017). The establishment of this capability has enabled a common picture of the EU's conduct of missions through cooperation with the existing civil structure, the Civil Planning and Conduct Capability (CPCC), their work being coordinated through a common support cell.

Furthermore, as a result of measuring progress, it was found that better cooperation of EU states on defence expenditure is needed, with no common vision being taken at national level. Eloquent are in this regard the press release of the European Commission of 7 June 2017 in which *"it is estimated that the absence of cooperation between Member States in the field of defence and security costs* *the Union between EUR 25 and 100 billion annually. 80% of public procurement procedures and more than 90% of research and technology activities are managed at national level. Up to 30 % of defence expenditure could be saved each year by pooling public procurement"* (A European Defence Fund, 2017) and the Munich 2017 security report that outlined *"the fragmented defence approach leads to unnecessary duplication and affects the deployment capacity of defence forces. There are 178 different weapons systems in the EU, compared to 30 in the US. There are 17 different types of battle tanks in the EU and only one in the US"* (Ibid.). The launch of the European Defence Fund on 22 June 2017 is the optimal solution to resolve state cooperation in defence spending and optimise EU costs in this area.

Complementing initiatives to strengthen member states cooperation in the field of defence is achieved by the implementation of the Coordinated Annual Review on Defence (CARD) Process, the European Council on 19-20 October 2017 marking the launch of the its test. Its role is to achieve a holistic picture at Union level on defence expenditure, member states investments and research-specific expenditure, thus being able to identify deficits and draw new directions of action to complement them, visible transparency and closer cooperation between member states on security and defence security, and effective defence expenditure planning.

Cooperation continued, with 32 new proposals for concrete actions in the early December 2017 process being approved during a parallel process at EU and NATO level concerning: counterterrorism, peace and security and military mobility.

An important step towards achieving the security and defence issue is the creation of the Permanent Structured Cooperation which is, in fact, a plan for closer cooperation in the field of defence, signed on 11 December 2017 by 25 countries within the European Union. The main aim of PESCO, which MEP Michael Gahler said to be the *"the central institution to ensure that the current isolated strands of military cooperation are put together under one roof"* (European Parliament), is to achieve close cooperation in the field of defence by combining resources and jointly developing combat and armaments, reducing the gap in the provision of technology and armaments between member states and achieving interoperability between the armed forces of members representing secondary objectives. An initial number of 17 projects were agreed in areas such as training, capability development and operational readiness in the field of defence, as follows: the creation of a European Medical Command; the development of secure and common technologies for European military radio equipment; the creation of a network of hubs for coordination and logistics supply throughout the EU; creating a concept of military mobility within the Union; the establishment of a Training

Centre for the European Mission; the establishment of a Certification Centre for the armies of EU Member States; developing operational energy sources that can be used in camps; the establishment of a capability of military specialists that can be used in a short time to limit the consequences of natural disasters, pandemics and calamities; the development of autonomous systems capable of operating underwater, land or air as countermeasures for maritime mines; the establishment of a martime capability to ensure better supervision and protection in the maritime environment; development of existing maritime surveillance systems; creating a platform for managing Cyber incidents; creating Cyber Incident Rapid Response Teams; establishing a Strategic Command and Control System for CSDP missions; developing a prototype for a European combat vehicle, such as a multirole platform; the development of a European mobile artillery platform and the creation of an Operational Crisis Response Command (EU Council, 2019).

The implementation of the measures is made transparent at the level of the two organisations, measuring in real time the results achieved and the need to develop new directions. In this regard, the European Council of 28-29 June 2018 highlights the significant progress made in the field of security and defence cooperation, stressing the need for further projects under PESCO and NATO-EU cooperation. It also identifies the need to speed up the implementation of the European Defence Industrial Development Programme, as well as to make further progress on the implementation of the European Defence Fund, the need to adopt new restrictive measures on the use and proliferation of chemical weapons, and the need to strengthen capabilities to combat cyber threats from outside the EU. Furthermore, the conclusions of the Council *"call for further deepening of EU-NATO cooperation, in full respect of the principles of EU inclusion, reciprocity and decision-making autonomy, including through a new joint declaration, building on the progress made in the implementation of the 2016 Joint Declaration and related action proposals"* (Ibid.).

The high level reached by EU-NATO cooperation was reaffirmed two days before the NATO Summit in Brussels, President Donald Tusk, President Jean-Claude Juncker and NATO Secretary-General Jens Stoltenberg signing a new EU-NATO Joint Declaration on 10 July 2018, eloquent in this regard being its first paragraph: *"Two years ago in Warsaw, we came together to strengthen EU-NATO cooperation aiming to promote peace and stability in the Euro-Atlantic area. Our respective efforts are mutually reinforcing, have improved the security of our citizens and strengthened our trans-Atlantic bond. Our longstanding cooperation has developed substantially, and is now unprecedented in its quality, scope and vigour. We share the same values* *and resolve to address, hand-in-hand, the common challenges we face. As our security is interconnected, we meet today in Brussels to reaffirm the importance of and the need for cooperation, and underline that our security and defence initiatives benefit each other"*. The document sets out a common vision of how the EU and NATO will work together to deepen partnership and counter common security threats and sets out the following areas on which the cooperation effort will continue to be focused: military mobility, cybersecurity, hybrid threats, counter-terrorism, women, peace and security.

The EU's progress in security and defence continues with the adoption, on 19 October 2018, of an updated list of projects to be developed under PESCO, with the number increasing from the 17 projects on 6 March 2018 to 34 projects. These include: training helicopter crews to operate in *"Hot and High"* environments; the establishment of a Joint Information School; the creation of Testing and Evaluation Centres; the development of non-human, multirole, threat-resistant terrestrial, multirole-resistant systems, which constitute the platform for transport, ISR, UAV capabilities, and other types of sensors; the creation of a European medium-range missile system; the development of a modular combat asset capable of performing the full spectrum of underwater defensive operations; the construction of a Eurodrone; modernisation of the European TIGER Mark III attack helicopter; developing a system of modular systems with dedicated command and control capabilities to combat the mini and micro UAV threat; development of ISR capabilities mounted on balloon platforms; the creation of a deployable command post for special forces operations to conduct low-intensity operations; creating a CBRN Surveillance Service with sensors to enable CBRN Recognised Picture; creating the concept of colocation in bases during operations; the development of a geo-meteorological and oceanographic coordination element; developing a network to monitor the alien space and warn against natural or other threats that may be generated by the human race and others (EU Council, 2019).

For unitary development, in parallel with the measures taken in the military sphere of security and defence, civil CSDP consolidation is also taking place, with the Civil CSDP Pact approved in December 2018. With this pact, the EU is strengthening the civilian crisis management capacity by: *"strengthening the police, the rule of law and civil administration in fragile and conflict contexts"* (Ibid.).

One year after the implementation of PESCO, on 14 May 2019, the EU Council assesses the progress made. Increased defence budgets and joint investment in this area, the increasing use of EU instruments, means and mechanisms for national defence planning are the most significant positive findings. At the same time, member states are encouraged to participate actively in cooperative capability development initiatives and to develop their capacity and deployment capacity. Measures need to also be taken to quickly and effectively implement PESCO projects, the vast majority of which being priorities of both the EU and NATO.

On 12 October 2019, 13 new projects are launched within PESCO (creation of an Integrated Training and Simulation Centre; creation of a European Cyber Academy, creation of a Medical Training Centre for special operations forces; construction of a CBRN Defence Range; creation of Divers Training Centres; construction of remotely piloted anti-submarine systems; creation of a prototype European corvette vessel; creation of jamming assets for airborne operations; creation of a Cyber Coordination Centre; the creation of air warning and interception systems; creating a modelling and simulation architecture to analyse how remotely piloted aerial systems are integrated into airspace) (Ibid.), total PESCO projects amounting to 47. Two months later, based on assessing progress in combating threats and minimising hybrid risks, the Council sets out the directions to be taken for the EU and the necessary guidance for further cooperation in this area.

CONCLUSIONS

Although the issues are presented succinctly, aware that in order to understand the whole phenomenon of EU-NATO cooperation, an in-depth analysis is needed, the results of which cannot be contained in a few pages, the full EU's dedication to the implementation of the joint actions established in cooperation with NATO and in the development of PESCO projects, in conjunction with the adaptation of its organisational and functional structure, reveals a much more active Union, eager to polish all its sides in order to take its well-deserved place in this security and defence puzzle, not only at regional level, but even globally.

Started more than 15 years ago, through the multitude of areas and projects jointly addressed, perseverance in respecting the principles and ideas promoted from the time of genesis to the present, success achieved in maintaining security and stability at regional level and even at global level, the EU-NATO partnership represents the most important and successfull form of cooperation of the beginning of the 21st century, in the form and extent that is expected to reach it in the future, probably for the entire century.

Since the beginning of cooperation, political dialogue between the EU and NATO has increased to a remarkable level in terms of consistency, transparency and clarity. High-level representatives from the two major organisations attend each other's most important meetings, which is confirmed by the consistency in the declarations issued in recent times. Staff and structures with the same specificity are jointly and increasingly working through the exchange of information and experience, cross-participation in working groups to find optimal solutions in all areas subject to cooperation. Since the outbreak of the pandemic, the EU and NATO have closely coordinated their respective efforts in overlapping areas of competence both at political and functional levels.

The joint capacity to act in the field of countering hybrid threats has increased through participation in joint exercises, conducting seminars and working groups on various topics on types of hybrid threats in the organising-participant system and subsequent change of roles within organisations, permanent horizontal exchange of information between staff, exchange of information process products, development of the warning system along the line of execution of hostile information activities, disinformation and others. In this respect, the eloquent is the cooperation between the EU Hybrid Fusion Cell, NATO's Hybrid Analysis Structure and the Helsinki Centre of Excellence, between the European External Action Service and NATO's Public Diplomacy Division, as well as between the Eastern Strategic Communication Centre of the European External Action Service and NATO's Centre of Excellence in Strategic Communication.

Progress has been made in the operational cooperation inclusive in the maritime field, too, through the ongoing exchange of information and participation in joint briefings at headquarters level, as well as through operational and tactical cooperation between the two organisations during operations in the Mediterranean and Aegean Seas. The EU and NATO continue to lead the Common Mediterranean Warning and De-conflict Mechanism (SHADE MED) as the main forum for improving situational awareness and the exchange of experience in order to improve de-conflict and coordinate efforts. Relevant for this area is also the joint participation in operations such as EUNAVFOR MED SOPHIA, SEA GUARDIAN and EUNAVFOR MED IRINI.

Cooperation in the field of cyber security and defence has been extended and improved by: informal exchanges of information on courses and forms of training in the field; mutual participation in cyber exercises; carrying out mutual exchange of information on specific concepts and doctrines; participation in joint briefings and workshops.

In terms of defence capabilities, efforts continue to ensure consistency of results between the 2018 EU Capability Development Plan (CDP), the Annual Coordinated Defence Review (CARD) and respective NATO processes, such as the NATO Defence Planning Process (NDPP) and the Partnership for Peace Planning and Review Process

(PARP). Consistency was further pursued in the implementation of projects under PESCO, with 38 of the 47 current projects also broadly addressing NATO's priorities. In addition, contacts at all levels have helped to ensure mutual awareness of ongoing activities within each organisation. Progress has been made in the implementation of the Military Aviation Strategy, cooperation within the NATO-EUROCONTROL Air Traffic Security Management Coordination Group and cooperation in the field of military mobility.

The development of cooperation in the field of defence industry and research has mainly improved through the exchange of information and experience between staff and structures with specific responsibilities within the two organisations in the field of: defence industry, standardisation, energy, CBRN, maritime research and not least artificial intelligence. Progress has been made in cooperation between the European Defence Agency (EDA) and the NATO Innovation Centre of the Allied Command Transformation (ACT) and NATO's Science and Technology Organisation (STO), with STO participating in maritime research projects.

Through joint participation in the exercises and the implementation of the lessons identified during their deployment, the framework was created to increase procedural and action altogether between the structures within the two major organisations. The exchange of experience was also achieved through mutual participation in symposiums on various topics, as well as through the involvement of staff during the planning of the exercises. Edifying in this regard are the participation of EU staff in NATO exercises such as CRISIS MANAGEMENT EXERCISE 2019 (CMX19), Coalition Warrior Interoperability Exercise 2019 (CWIX19), TRIDENT JUPITER 2019 and TRIDENT JACKAL 2019 and the participation of NATO staff at the EU DARK BLADE 2019, MILEX 19, EU CHEM REACT and the EDA Helicopter Tactics Symposium.

Open dialogue and transparency of actions have facilitated actions that have led to de-conflictisation and coordination of efforts in the following main areas: good governance, strategic communication, CBRN, counter-terrorism, women, peace and security.

To conclude, the future of EU-NATO cooperation will continue to focus on dialogue, transparency and full involvement in both directions, in complementarity, synergy and full respect for the institutional framework and decision-making autonomy of both actors, aiming at meeting the full set of joint actions set out in the agreements concluded, as also presented in the text of the report: *"While the implementation of the 74 common proposals is based on regular, close and pragmatic staff-to-staff engagement, continued full engagement and support* *by the NATO Allies and the EU Member States remains crucial. In this context and in light of known and new challenges, such as the COVID-19 pandemic, it is more important than ever that the EU and NATO continue to consolidate and further strengthen their close and mutually reinforcing cooperation and strategic partnership for the benefit of the Euro-Atlantic security and their members”* (EU Council, 2020).

BIBLIOGRAPHY:

1. Bădălan, E., Frunzeti, T. (2003). *Forțe și tendințe în mediul de securitate European*. Sibiu: Editura Academiei Forțelor Terestre *“Nicolae Bălcescu”*.
2. Bogzeanu, C. (2011). *Rolul NATO și UE în managementul crizelor în Balcanii de Vest*. București: Editura Universității Naționale de Apărare *“Carol I”*.
3. Idem. (2013). *Evoluția relației NATO-UE față de determinarea polilor de putere*. București: Editura Universității Naționale de Apărare *“Carol I”*.
4. Buzan, B. (2000). *Popoarele, statele și teama*. București: Editura Cartier.
5. Duțu, P., Bogzeanu, C. (2011). *Reforma instituțională a UE din perspectiva Politicii de Securitate și Apărare Comune*. București: Editura U.N.Ap. *“Carol I”*.
6. Horoșanu, G. (2014). *NATO-UE a smarter collaboration*. București: Editura Tritonic.
7. Mureșan, M., Țenu, C., Stăncilă, L. (2006). *Securitatea europeană la începutul mileniului 3*. București: Editura Universității Naționale de Apărare *“Carol I”*.
8. Pavel, Gh. (2007). *Mediul de securitate european și euroatlantic*. București: Editura Universității Naționale de Apărare *“Carol I”*.
9. Stoica, Al. (2014). *Marii actori statali și Uniunea Europeană în competiția globală de interese*. București: Editura Universității Naționale de Apărare *“Carol I”*.
10. Cologne European Council (1999). Conclusions of The Presidency, https://www.europarl.europa.eu/summits/kol2_en.htm#an3, retrieved on 11 September 2020.
11. European Comission (2017). *A European Defence Fund: 5.5 billion EUR per year to boost Europe’s defence capabilities*, https://ec.europa.eu/commission/ presscorner/detail/ro/IP_17_1508, retrieved on 11 September 2020.
12. Consilium Europe (2003). *European Security Strategy: A Secure Europe in a Better World*, https://www.consilium.europa.eu/ro/documents-publications/publications/european-security-strategy-secure-europe-better-world/, retrieved on 2 October 2020.
13. Consilium Europe, (2020). *European Union Cooperation in Security and Defence*, https://www.consilium.europa.eu/ro/policies/defence-security/, retrieved on 11 September 2020.
14. Consilium Europe (2018). *European Council Final Conclusions*, https://www.consilium.europa.eu/media/35954/28-euco-final-conclusions-ro.pdf, retrieved on 11 September 2020.
15. Consilium Europe (2018). *Joint UE-NATO Declarațion*. Brussels. https://www.consilium.europa.eu/media/36096/nato_eu_final_eng.pdf., retrieved on 11 September 2020.

16. Consilium Europe, Fifth progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017, https://www.consilium.europa.eu/media/44451/200616-progress-report-nr5-eu-nato-eng. pdf, retrieved on 11 September 2020.
17. Consilium Europe (2020). PESCO-Project. https://www.consilium.europa.eu/ media/41333/pesco-projects-12-nov-2019, retrieved on 11 September 2020.
18. Consilium Europe (2017). EU Defence Cooperation, https://www.consilium.europa.eu/ro/press/press-releases/2017/06/08/military-mpcc-planning-conduct-capability, retrieved on 11 September 2020.
19. Consilium Europe (2018). Civilian Common Security and Defence Policy, https://www.consilium.europa.eu/ro/press/press-releases/2018/11/19/civilian-common-security-and-defence-policy-eu-strengthens-its-capacities-to-act/, retrieved on 11 September 2020.
20. Consilium Europe (2016). Taking EU-NATO cooperation to a new level, https://www.consilium.europa.eu/en/press/press-releases/2016/12/13/tusk-juncker-stoltenberg-opinion/, retrieved on 11 September 2020.
21. DEX (1998). *Dicționarul explicativ al limbii române*. București: Editura Univers Enciclopedic.
22. EEAS (2016). *A Global Strategy for the Europeen Union’s Foreign and Security Policy*.
23. European Defence Agency, Mission, https://www.eda.europa.eu/Aboutus/Missionandfunctions, retrieved on 11 September 2020.
24. North Atlantic Treaty Organisation (2002). EU-NATO Declaration on ESDP. http://www.nato.int/cps/en/natolive/official_texts_19544.htm., retrieved on 11 September 2020.
25. European Parliament (2017). News, Pesco: EU countries sign off on plan for closer defence cooperation, https://www.europarl.europa.eu/news/en/headlines/security/20171208STO89939/ pesco-eu-countries-sign-off-on-plan-for-closer-defence-cooperation, retrieved on 2 October 2020.
26. EUR-LEX, Treaty of the European Union (consolidated version), Protocols, https://eurlex.europa.eu/legalcontent/RO/TXT/HTML/?uri=CELEX: 12012M/TXT&from=EN, retrieved on 11 September 2020.
27. European Security Strategy (2003), EU Council. Brussels, https://data.consilium.europa.eu/doc/document/ST-15895-2003-INIT/en/pdf, retrieved on 2 October 2020.

NATO-EU PARTNERSHIP – AN IMPORTANT STEP TOWARD ACCOMPLISHING GLOBAL SECURITY –

Lieutenant Petru-Viorel ENE, PhD

Ministry of National Defence, Romania

After almost 72 years of existence, the North Atlantic Treaty Organisation brings together 30 states with common values and aspirations, setting side by side Europe and North America. If in the moment of its foundation the Alliance faced a limited range of risks, today the Organisation is confronting with a wide range of threats, from terrorism to cyber-attacks.

In this context, a strong transatlantic partnership and, implicitly, a close cooperation between the European Union and the North Atlantic Treaty Organisation are necessary to strengthen the security climate, especially considering the fact that the two organisations have 22 European states in common. The security challenges are gaining new valence, so the response must be combined to further ensure the transatlantic security and peace. Will the North Atlantic Treaty Organisation and the European Union succeed in making the transition from a transatlantic to a global peace?

Keywords: NATO; EU; democracy; strategic partnership; cooperation;

INTRODUCTION

In these difficult times in which the world's states are facing all the problems generated by the coronavirus pandemic, we notice, perhaps more clearly than before, that without a strong alliance on which to lay the foundation of a strong relationship between partner states, there is no possibility to deal with political, social, financial, medical and security pressures.

Solidarity must be at the heart of the international architecture. In this way, through the powerful effect of teamwork, through the permanent exchange of information and capabilities, through the combined effort of all the states, we can develop a more secure, prosperous and free society.

The most important role in this approach is played by international organisations, considering, on the one hand, the fact that their very structure is based on the pillars of democracy, prosperity, solidarity, and, on the other hand, the resilience that they have shown over the past decades.

In hindsight, it is clear that we can no longer analyse all the things only at a regional level, without taking into account the whole picture, because the political changes and all the implications we feel today are gaining global valences, and the states are, more than ever, in an obvious interdependence.

The detachment from a conventional type of war by adopting hybrid methods of attack, the vital cyberspace in a modern society, and the practices by which different countries intervene in the internal affairs of other states, represents a set of risk which are very difficult to manage by a single state. This is why, since the early 1990s, there has been a permanent need to strengthen the international cooperation.

In this regard, given the international climate with its unprecedented challenges, the cooperation between the European Union (EU) and the North Atlantic Treaty Organisation (NATO) was seen not only as an important step in ensuring the security of the allied states, but also as a necessary measure to implement.

Today, the security challenges can easily outweigh the ability of a single state to defend itself. Whether we are talking about terrorism, the proliferation of weapons of mass destruction, organised crime, climate change, natural disasters, or even if we are focusing on the analysis of cyber-attacks, fake news, sanitary crisis like a pandemic, dealing successfully with all these threats must be the result of the combined effort of the EU and NATO states.

Of course, the United Nations also plays a key role in this, given its active involvement in security, peacekeeping operations, the development of harmonious relations between states and the ongoing desire for international cooperation. However, in this approach, we will turn our attention only to the NATO-EU partnership.

At the NATO Summit, held in Warsaw in 2016, through the joint declaration of the Secretary General of NATO, the President of the European Council, and the President of the European Commission, the partnership between NATO and EU got strengthened, and the cooperation process gained new approaches in strategic areas, including hybrid threats, maritime security and cyber security.

This statement came as a natural consequence of the fact that both structures were facing similar challenges and sharing common interests (EU-NATO Cooperation, 2016, point 1), as arising from the priority fields assumed at the Warsaw Summit.

We can say that the European Union and NATO are interconnected, given the need to ensure a secure climate and the right conditions for the development of its citizens prosperity. Not only that 22 EU member states are aligned under the umbrella of NATO, but both values and security threats call for the combined action of the two international structures.

The 21st century has put NATO in the position to re-evaluate the definition of security and the means needed to guarantee it. Thus, security can no longer be limited to the military capabilities that the Organisation can make available in order to repel an armed attack, but must take into account the unseen enemy, the non-military dimension and all the social, cultural, religious and ethnic factors (Pasăre, 2014).

The complementarity must be the key word in this endeavour, and the interoperability between these two organisations must be constantly raised to a new level, in order to provide security for all the member states and, why not, for all mankind.

NATO AND EU PREMISES

In order to understand the need for cooperation between the two organisations, it is necessary to make a sketch of the most important historical events that have led to the establishment of these international structures. Although each of them has its own peculiarities, there are some similarities in terms of purpose and the premises of their very existence.

At the end of the World War II, with about 36 million citizens killed in the conflict (A Shorth History of NATO), Europe was on its knees. Like it was not enough, the desire of the Soviet Union to maintain its influence in the Eastern part of Europe, the economic and humanitarian crisis put a huge pressure on the shoulders of the old continent.

Thereby, after a long period in which they practiced an isolationist policy, determined by the fear that Europe will return to the same policies that led to the world war, the United States decided to become actively involved in the European political life.

Even though the US aid, through the implementation of the Marshall Plan (Kagan, 2015, pp. 48-50)[1], was the cornerstone of European reconstruction, European states still felt the need to strengthen their security through military, economic cooperation and political progress[2].

This reality was confirmed by the conclusion of the Treaty of Dunkirk between the United Kingdom and France, signed on 4 March 1947. Through this treaty, the signatory states undertook to provide mutual support in the event of an aggression by Germany, in order to prevent it from becoming again a threat to the European peace and to strengthen the existing economic relations (Zlătescu, Bulgaru, 2016, p. 7). This Treaty was to be the cornerstone of the North Atlantic Treaty Organisation.

Signed in Washington on 4 April 1949 by the United States, Canada and other 10 European states (Belgium, Denmark, France, Island, Italy, Luxembourg, Norway, the Netherlands, Portugal, the United Kingdom), the North Atlantic Treaty Organisation was born. As a politico-military alliance, the Organisation was established to respond to the Soviet expansionism, to prevent the rebirth of militarism and radical nationalism through a consistent North American presence, and to encourage the European integration policy.

The provisions of the Treaty revolve around Article 5, which states that the allied States undertake that an armed attack on one or more members is an attack against them all. Consequently, in the event of such an armed attack occur, the response in order to restore and maintain the transatlantic security must be a combined one. In this endeavour, singing the Treaty was the first step in strengthening the transatlantic cooperation. At the same time, it was the moment where the foreign policy of the United States underwent significant changes, becoming part of the global community.

If, at first, NATO was only a politico-military alliance that did not have the necessary means to ensure the regional security, this changed soon. The detonation

[1] By consolidating European economy, the USA met two important goals: to have an economic partner and to strengthen the European defence capability against the Soviet Union.

[2] In this respect, the Western European Union was established – an international military organisation based on the principle of collective defence and with the purpose to facilitate the economic, social and cultural cooperation between Member States (https://www.britannica.com/topic/Western-European-Union).

of the first Soviet atomic bomb, on 29 August 1949, and the outbreak of the Korean War in 1950, led the Alliance to realise the need for immediate regrouping and the need for accelerating the efforts to ensure a combined response and regional security.

Therefore, following the events of 25 June1950, when without any warning, the North Korean army, supported by the Soviet Union, crossed the 38th[3] parallel and attacked South Korea, the United States understand the necessity for international cohesion, for a mass production of military equipment to discourage the Soviet Union and to sustain the Alliance member states.

As a result, NATO consolidated its command structure, established the Supreme Command of the Allied Forces in Europe, in the suburbs of Paris[4] and in February 1952 appointed the first Secretary General, in the person of Lord Hastings Lionel Ysmay.

The great victory of the Korean War, officially concluded in 1953, would be the birth from the ashes of the conflict of the United Nations, as the first international organisation that managed to repel an armed attack against a peaceful country (van Loon, 2017, pp. 522-526).

On the other hand, in this not very friendly context, but under the umbrella of the transatlantic security, managing to stabilise the balance in the political, economic, and humanitarian crisis, enjoying the consistent help from the United States, the Western Europe began to regain its radiance.

The extreme nationalism led to four wars between French and Germans, two of which were the World Wars. It was clear that a new paradigm had to be adopted, so the need to implement measures aimed to build a supranational entity was highlighted.

The shaping process of the supranational structure was, therefore, the response of the Europeans to the interwar period, characterised by unpredictability, by hazard, by the cruel and degrading socialist, communist governments. Moreover, in the context of the crisis that the European states were acting against, the need for refurbishment, economic cooperation and the expansion of the political relations was more prevalent than ever (Marr, 2015, pp. 577-580).

[3] Established in Yalta as the delineation between North Korea – influenced by the Soviet Union and South Korea – by the United States of America.

[4] Following the split between France and NATO's military structure, in February 1966, the Allies moved quickly to find new hosts for the headquarters that would have to leave France. They decided to move NATO's political headquarters from French territory as well. Belgium became the host nation for both NATO and SHAPE, on 26 October 1966, the decision being made to establish NATO's new location in Brussels.

Europe's decline was a wake-up call at both political and academic level. Thus, the interwar period was perceived as the period when Europe stopped having a strong voice in the world. The command of the world was to be taken by the United States, the shift of the power pole being obvious.

The most feared consequence of this decline was the departure of the European states from a set of common values and the increasing influence of the Soviet Union over the old continent. It is about that pseudo-concept of José Ortega Y Gasset, the man-mass, which promotes the vehement refusal to acknowledge a higher entity, a mentality taken over at state level and manifested by moving away from civilisation, from the European doctrine.

At the same time, the Spanish philosopher pointed out that this apparent European decline would be the most precious moment that would allow Europe to reinvent itself, to reborn, to evolve, and to lay the very foundation stone for what would later be the European Union (Gasset, 2007, p. 171).

Of course, these theoretical concerns, which we find in the interwar period, represented only the first step on the path to a consolidated European identity, concrete political steps being mandatory, in accordance with the historical reality that European states witnessed. These political manifestations represented the willingness of the European states to strengthen, to regroup in an entity that would ensure peace, as well as economic and social progress.

It should be pointed, from the outset, that the purpose of the Communities was to unify all the European states through universally applicable legislation, through common policies, a single currency, standards and values shared by all member states.

An important step in this direction was the moment of 23 July 1952[5], when the Frenchmen Jean Monet and Robert Schuman`s proposal, known as the Schuman Plan, was put into practice – six countries (Belgium, France, Italy, Luxembourg, the Nederland, and West Germany) joined together and formed the European Coal and Steel Community.

Among the reasons behind the founding of these communities we mention the economic unification, the establishment of a European federation, the production process modernisation, and above all, the elimination of the secular opposition

[5] On that date, the founding Treaty of the European Coal and Steel Community, signed in Paris on 18 April 1951, entered into force. The preamble to the Treaty shares common characteristics with those of the North Atlantic Treaty. Thus, world peace is mentioned as well as the achievement of this goal through adapted efforts to the existing dangers. Moreover, a *de facto* solidarity that would constitute the premise of a common economic development is envisaged.

between France and Germany by establishing an international control mechanism over the basic branches of the armament industry (Fuerea, 2016, pp. 19-20).

Moreover, in 1954 the Western European Union was founded as a legacy of the fact that the Western states opposed the Soviet expansion, understating the need for a common front, and, on 1 January 1958, the well-known European Economic Community was created, known as the Common Market, and the European Atomic Energy Community/Euratom.

The economically fruitful cooperation, by ensuring the free movement of workers and capital, and, at the same time, the possibility to exercise the security control over the destination of the products available on the nuclear market came into force within a political alliance embraced by 28 countries and which brought back the European states brilliance, prosperity, and common purposes (van Loon, p. 529). Even so, the European goal of merging nations and the focus on the rule of law, the supremacy of human rights have proven to be insufficient in the current geopolitical configuration.

If, on the one hand, the European aspirations to regroup under the umbrella of the same values evokes the world's admiration and shows that dialogue must be a valuable weapon in solving any disputes, on the other hand, the non-participation in security as an independent entity, with armed forces capable to provide security for the citizens of the members states, in a constantly changing world, in which new threats emerge, has been seen as a weakness, not only by citizens, but also by officials (Meixler, 2018).

COMMON VALUES, COMMON FUTURE

From the Preamble, the North Atlantic Treaty presents the main pillars on which the Alliance was established. Thus, the signatories of the treaty affirm their desire to live together in peace, commit to defend the individual freedom, the principles of democracy and to obey the laws. At the same time, Member States commit to promote the stability and the welfare of the North Atlantic region.

Further, Article 1 provides the obligation for the Member States to not endanger the security and to respect the international law. Article 2 complements Article 1, in the sense that, the Parties will contribute to further development of peaceful and friendly international relations, to promote the conditions of stability and welfare, and to encourage economic cooperation between any or all of them (North Atlantic Treaty, 1949).

On the other hand, the Treaty establishing the European Coal and Steel Community, emphasises, from the beginning, that world peace can only be achieved through efforts adapted to the existing dangers, and that Europe's role in achieving this goal is undeniable.

At the same time, the need for the facto solidarity between Member States and a strong economic development through the establishment of development relations are the basic principles of this Treaty (Traité instituant la Communauté Européenne du Charbon et de l'Acier, 1951).

The European Economic Community and the European Atomic Energy Community Treaties, were grounded, on the one hand, on a common commercial policy, a custom union, a strengthened economic and social environment, technological development and common policies in areas such as agriculture, fishing or transportation[6], and on the other hand, on a common nuclear industry market, to exclude the possibility of an armed conflict between European states and to ensure their cooperation[7].

In our analysis, the Maastricht Treaty, signed on 7 February 1992, known as the Treaty of the European Union is highly important. The Treaty represents a new stage in the process of consolidation of a united Europe, with common goals and ideals. Therefore, the most important objectives that the Union set itself are to promote economic and social progress, the common security and defence policy, human rights and the best interests of the Member States, and to develop close cooperation on justice and home affairs.

We have made this assessment of the principles and objectives on which NATO and EU exist precisely to emphasise that they have common premises, a common trajectory, common beliefs and visions. Both organisations are extremely careful about promoting and ensuring the security and the prosperity of the citizens.

It is clear that the most important values of the two organisations can only be common, given their composition and the entire historical development. Therefore, the cooperation between them is not only desirable but absolutely necessary.

The direct involvement of the European Union in the regional security must not have the character to exclude or compete with NATO, on the contrary, it must be achieved through a cooperative activity.

The existing common defence and security policy at European Union level is of great help to the Alliance, as long as their efforts are complementary and do not overlap with NATO programmes and capabilities.

The European contribution to the common security must rely on effective policies, in order to achieve the planned results. The European Union common

[6] As regards the European Economic Community.

[7] Regarding the European Atomic Energy Community.

security and defence policy, which establishes the necessary framework for political and military structures for the purposes of enforcement the Union's military and civilian missions and operations outside its borders, is an important step in the two international organisations` efforts to secure the regional security through joint effort, cooperation and ongoing dialogue.

If we look at the military spending at European level, we see that although Europe is a major player in the field, because of inefficient spending, lack of interoperability and technological gaps, there is a considerable discrepancy between the existing capabilities and the possible outcome if all these security policies would have a common ground.

In other words, without a sustained, coordinated and effective investment, Europe's ability to ensure the security will suffer. In this direction, cooperation, interoperability, development of long-term perspectives and participation in joint NATO-EU operations are elements of utmost importance.

However, why is the cooperation policy between the two organisations preferable to competitiveness? Well, the international architecture defined after the World War II is full of challenges from every dimension of our existence.

The complexity and unpredictability of the attacks, the fact that they are not limited to a physical space, their frequency and profound implications, the peculiarities that the European Union presents, the growing pressure from Russia, China's aspirations of becoming a global leader, the refugee crisis are some of the reasons why cooperation is indispensable.

Organised crime, climate threats, interethnic conflicts are other examples to emphasise that no state, no organisation can solve all the problems by acting alone. Partnerships are necessary, perhaps more than ever, in order to ensure global peace and a security climate, because the emergence of all these challenges is impossible to predict, to anticipate, and an optimal response can only be achieved within a strong alliance.

The importance of cooperation between EU and NATO becomes apparent, on the one hand, from the joint actions in Kosovo, Afghanistan, Iraq, and Bosnia and Herzegovina, on the other hand, from the permanent exchange of policies and good practices in various key areas.

As a consequence of the cooperation missions, the EU and NATO signed the Berlin Plus Agreement, with the aim of increasing the level of interoperability and of streamlining cooperation between the two organisations, with the EU acquiring the right to use NATO's capabilities. It is therefore an agreement on the logistical support which is necessary for the good cooperation and which highlights the need for cooperation in strategic areas.

In this regard, we mention areas such as cyber security – the WannaCry attack, military mobility, hybrid threats[8], mutual participation in exercises, such as CYBRID, an exercise organised by the European Union in Estonia in the field of hybrid threats, the Cyber Coalition, NATO's annual exercise, and the Operation Sea Guardian, aimed at fighting against illegal migration, arms and human trafficking, and to strengthen the security of maritime borders. These important joint exercises enable both structures to know each other's working methods better, to reinforce the coordination capacity in order to achieve the common strategic objective.

However, in this hostile environment with diverse security risks, the cooperation between the two entities in the field of security must be accompanied by the extension of these relations and enhanced cooperation with African and Asian states, with African Union member partners, Arab League and not only.

The European Union and the North Atlantic Treaty Organisation have the vocation to ensure global peace and, afterwards, to provide the transition from transatlantic to global security. The eradication on any regional conflict, the progress, the ongoing cooperation and the mutual trust are some significant elements in this regard.

It is clear that, in order to strengthen a global security climate, the preconditions for a permanent military and political cooperation must be created, in which the footprint of both organisations to become more noticeable.

Therefore, the impact of the adopted policies in the transatlantic cooperation must go beyond the geographical boundaries covered by the two organisations and must be mastered and applied globally. It is the safest way to ensure a secure climate for all the citizens, regardless of the state in which they live or the challenges they are facing.

The North Atlantic Treaty Organisation and the European Union strive to ensure transatlantic peace, the respect for common values, for individual freedoms, for democracy, for human rights and to promote the rule of law.

The ongoing challenges facing the two international organisations have the character of destabilising, of jeopardising the work and the progress made during all this time. Moreover, the engagement in fighting against all the threats may also be difficult to reach if we take into account the diverse and sophisticated nature

[8] Both international structures contribute to and benefits from the facilities offered by the European Center of Excellence for Combating Hybrid Threats in Finland.

of the new types of challenges. The response to all existing challenges must also include non-EU actors for a course of action tailored to each threat.

In this regard, NATO and the EU have not only committed themselves to provide territorial protection for the allies, but have also worked to protect and promote their core values, crisis prevention and crisis management as well as post-conflict stabilisation and reconstruction. These joint steps were preceded by extensive negotiations and various policies in order to enable the accomplishment of such common actions.

Just like the EU-NATO partnership has gone through several stages of development until it reached the necessary conditions for cooperation and interoperability, likewise it is necessary to develop relations with Asian and African states through joint actions in priority fields, in order to strengthen the dialogue and to establish a sustainable strategic partnership.

Therefore, to ensure the expansion of the security and prosperity climate from the regional to global level, the culture in the field of security cooperation must be constantly cultivated, and NATO-EU cooperation should become the pillar on which global partners can build an extended, common and lasting security environment.

Unfortunately, the instability of the Middle East has posed a series of real challenges for both EU and NATO member states, and the decisions taken by nations as independent entities have had a major impact on both organisations. Thus, the development of a sustainable, strengthened climate of peace that successfully meets all the external challenges must be endorsed through direct involvement, investments and permanent assistance, and has to include areas characterised by instability.

CONCLUSIONS

The European Union is the natural partner of the North Atlantic Treaty Organisation, and together, with the joint effort and complementary actions, have the vocation to expand the security climate globally.

As it has been mentioned before, NATO and the EU have ensured the Euro-Atlantic security environment and the prosperity of all the allies for more than 70 years, and almost 90% of the citizens of the NATO's allied states are European citizens. In this context, a strong Europe means a strong Alliance, so all the investments for the citizen's security represent common goals and shared achievements (Geoană, 2020, p. 42).

Moreover, these moments of unprecedented uncertainty that we are witnessing raise fundamental questions about the architecture of the world governance and about the need for a permanent cooperation and collaboration, not only at regional level, but also globally.

In this endeavour, it is important for Europe to remain at the heart of the transatlantic security, strengthening the Alliance's eastern flank through an increased military presence and extending its influence over Asian and African states.

The cooperation process outside the European soil is a long-term course of action and need to be strengthened, so that the Euro-Atlantic values can contribute to the creation of the necessary cooperation mechanism in order to ensure the transition from regional peace to global peace and security.

Of course, ensuring the security and the involvement of both EU and NATO in safeguarding global peace involves huge costs, thereby all the expenses must be efficient and in areas of high interest, such as cyber-attack response infrastructure and artificial intelligence.

With regard to the necessary funds in this field, the European Parliament has constantly encouraged Member States to meet NATO's capability targets, which requires a minimum level of defence spending of 2% of GDP, but meeting this condition has proved to be a lasting approach and it is a policy that, at the moment, is not approved by all the North Atlantic Organisation member states.

Regarding the efforts of both NATO and the EU, if initially they were parallel rather than convergent, today all NATO policies encompass the European political dimension. Achieving this goal has not been easy at all, however the joint effort of the two international entities has led to prosperity and regional peace. Thus, the next step in the NATO-EU partnership should be to extend the sphere of responsibility and their influence, so that Asian and African states can enjoy the values and the security environment that this partnership entails.

As the Brussels and Berlin Agreements state, the main principles of NATO and EU cooperation shall include interconnected actions and common capabilities available to both international organisations. Avoiding an unnecessary duplication of effort and interoperability are the fundamental mechanisms of the partnership.

A fine example in this regard is the necessity for common information, surveillance and recognition capabilities. On the one hand, if the EU acquires such a system, it must be available to both EU and NATO, and on the other hand, NATO's capabilities must be available for the EU, avoiding, in this way, any unnecessary investments (Lute, 2019, p.18).

In its mission of expanding the security climate, the North Atlantic Treaty Organisation has developed flexible cooperative relationships with partners from around the world. Whether we are talking about New Zealand, Pakistan or Iraq, about Japan or South Korea, the global partnership has characterised the Alliance's policy. At the same time, the Organisation consults with other non-member states[9] that have not concluded bilateral cooperation programmes at the level of the Alliance.

As an extension of the current bilateral relations between the two international organisations and non-member states, in order to initiate the cooperation process and to achieve an effective dialogue with Asian and African states, NATO and the European Union can launch policies in various fields such as the new security threats, fighting against piracy, energy security or aspects related to humanitarian disasters.

This type of flexible global cooperation policy needs to be implemented in future partnerships outside the transatlantic territory, and the consolidation process, the permanent dialogue and a strong partnership must involve the entire international community to reach the fundamental purpose of the international organisations, and the transition from transatlantic peace to global security to be achieved.

BIBLIOGRAPHY:

1. Fuerea, A. (2016). *Manualul Uniunii Europene*. București: Editura Universul Juridic.
2. Gasset, J.O.y. (2007). *Revolta maselor*. București: Editura Humanitas.
3. Geoană, M. (2020). *Stronger Together*. Brussels: European Defence Matters.
4. Kagan, K. (2015). *Lumea clădită de America*. București: Editura Humanitas.
5. Lute, D., Burns, N. (2019). *NATO at Seventy: An Alliance in Crisis*. Harvard Kennedy School.
6. Marr, A. (2015). *Istoria lumii*. București: Editura Nemira.
7. Meixler, E. (2018). *French President Emmanuel Macron Calls for a 'European Army' to Defend Against China, Russia and the U.S.*,https://time.com/5446975/emmanuel-macron-european-army-russia-us/, retrieved on 9 September 2020.
8. Pasăre, C.I. (2014). *Rolul României în îndeplinirea obiectivelor de securitate ale NATO*. Intelligence Journal.
9. Van Loon, H.W. (2017). *Istoria omenirii*. București: Editura Humanitas.
10. Zlătescu, I., Bulgaru, A. (2016). *Organizații europene și euroatlantice*. București: Institutul Român pentru Drepturile Omului.

WEB SOURCES:

1. A Short History of NATO, https://www.nato.int/cps/en/natohq/declassified_139339.htm, retrieved on 2 September 2020.

[9] China, India, Singapore, Indonesia.

2. European Council. EU-NATO Cooperation, https://www.consilium.europa.eu/media/21481/nato-eu-declaration-8-july-en-final.pdf, retrieved on 2 September 2020.
3. https://intelligence.sri.ro/rolul-romaniei-indeplinirea-obiectivelor-de-securitate-ale-nato/, retrieved on 28 September 2020.
4. https://www.consilium.europa.eu/media/21481/nato-eu-declaration-8-july-en-final.pdf, retrieved on 2 September 2020.
5. https://www.eda.europa.eu/docs/default-source/eda-magazine/edm19_web.pdf, retrieved on 2 September 2020.
6. https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:11951K/TXT&from=RO retrieved on 2 September 2020.
7. https://intelligence.sri.ro/rolul-romaniei-indeplinirea-obiectivelor-de-securitate-ale-nato/, retrieved on 28 September 2020.
8. https://time.com/5446975/emmanuel-macron-european-army-russia-us/, retrieved on 2 September 2020.
9. https://treaties.un.org/doc/Publication/UNTS/Volume%209/v9.pdf, retrieved on 28 September 2020.
10. https://www.britannica.com/topic/Western-European-Union, retrieved on 28 September 2020.
11. https://www.nato.int/cps/en/natohq/topics_49188.htm, retrieved on 2 September 2020.
12. https://www.nato.int/docu/review/2007/issue2/romanian/history.html, retrieved on 2 September 2020.
13. https://treaties.un.org/doc/Publication/UNTS/Volume%209/v9.pdf, retrieved on 2 September 2020.

SMART POWER – CHALLENGES AND OPPORTUNITIES FOR TRAINING AND EDUCATION IN INTELLIGENCE

Dorinel-Ioan MOLDOVAN
Ministry of National Defence

The article, starting mainly from the concerns of Romanian authors in the field, intends to highlight the importance of education and training in defining, building, supporting and designing a Smart Power strategic model, as a way to make optimal use of the resources and power tools a state has at its disposal for national interests, values, objectives and goals.

Currently, one of the relevant characteristics of the security environment is the quantitative domination of information. Its production, management, manipulation, multiplication and capitalisation transcend strictly institutionalised boundaries, and the effects are found in all areas of society.

In this context, the specific training and education of specialists in intelligence institutions, accepted as one of the power tools of states, takes place under the complexity of the evolution of information and means of transmission and processing, in socio-economic developments, including pandemics, as well as under the pressure of the dynamics of political debates and actions.

Keywords: hard power; intelligence; education; leadership; performance;

INTRODUCTION. SMART POWER – SHORT THEORETICAL APPROACH

Credited as one of the most important authors who has approached the concept of *"smart power"*, Joseph Nye (Assistant Secretary of Defense for International Relations in the Clinton Administration) starts from defining power as the ability of a state to achieve the desired results, including changing the behaviours of other actors, if the situation requires.

Frequently, power is associated with the possession of specific resources, generally associated with: population, territory, natural resources, economic means, military force; power knows a potential or a materialised dimension; through government policies whose success depends on skilled leaders and state leaders. Traditionally, the test of great power has been the constitution of the *"force for war"* (Nye, 2002, p. 4).

Nye details the distinction, differentiating between *hard power* (derived from military and economic instruments) and *soft power* (generated and sustained by the attractiveness offered by the culture, ideology, values, institutions of a state) as a phenomenon that depends on the degree or consistency of their use, both in the nature of the behaviour and in the materiality of the related tools and resources. Both types of power interact, support each other, and are aspects of the ability to achieve goals, by affecting the behaviours of other actors. As an example, *"command power"* is the ability to exercise authority (hard), to change what others do and resides in coercion or persuasion (induction). *"Co-optive power"* represents the capacity, the ability of a state to redesign, remake, influence and reformulate (*"shape"*) what other state actors want and can derive from the attractiveness of a culture and ideology, respectively from the ability to manipulate the political option agenda. Obviously, the forms of behaviour of states in the case of exercising power in international relations take place along a continuum, between the two extremes (the power to exercise authority, respectively to co-opt) and may include: coercion, persuasion, influencing the political agenda, attractiveness. From this perspective, there is a tendency to associate the resources specific to soft power with the behaviour attributed to co-opting power, while the resources associated with hard power are rather related to the behaviour of exercising command, domination, the relationship being, however, imperfect. As an example, some states may be more attracted to states that have the power to exercise authority, due to the myth of invincibility enjoyed by the latter; at the same time, authority can sometimes be used to set up institutions that later become legitimate. But, in general, the association presented above is the one that refers to the reference of soft and hard power. (Ibid., p.179).

In line with the argument, power in the global information age is becoming less tangible and less and less coercive, especially among advanced states. In a diverse world, such as today, all three sources of power, military, economic and soft remain relevant, in varying degrees of interaction and mutual influence, and if current economic and social trends are maintained, leadership in the information revolution and soft power will become increasingly important. The power in the 21st century will be exercised through a mix of hard and soft resources and tools. In this context, the USA will continue to employ more than any other state the three sources: military, economic and soft power, and the biggest mistake the USA could make in this context would be to fail in a one-dimensional approach and consider that investing exclusively in the military instrument will ensure and sustain American power. (Ibid., pp.11-12).

On the other hand, subsumed under the purpose of the topic and the article, considering the term SMART as an acronym, the literature in the field of organisation management proposes it as a usual, practical way to define managerial objectives: Specific Measurable Achievable/Agreed Relevant Timely. That is why, management, as a leadership structure, must consider a number of criteria for establishing and defining an organisational goal: to be specific, to refer to a specific field, to be clearly and precisely defined; to be measurable, quantifiable through the managerial tools available, to allow its evaluation (quantitative and qualitative) as objective as possible; to be able to be satisfied with the resources available to the organisation, taking into account, in particular, the human resource, with its qualifications, competences and characteristics and at the same time to be approved by the employees and management; to be relevant for the field of activity of the organisation and to contribute to the mission of the organisation, to be achievable in a concretely established time interval, to be framed in time. The multitude of specialised works in the field offers a special place to this way of approaching the objectives. Thus, the management's perspective on defining goals or objectives can be convergent to the ways of using the power tools available to politico-military or political decision- makers.

Promoted as a strategic model for the 21st century, smart power requires the elites of a state, especially the political class, to identify and materialise the characteristics of public institutions, define policies, implement and correct them in a timely manner, and involve all constituents of society in a national synergy, on two levels, domestic and international. Externally, the intelligent use of national power instruments requires the vision and action of state institutions, the national business environment, academia and civil society to identify those forms of participation and international cooperation and partnership through which national interests are supported, political objectives are achieved, and vulnerabilities, risks and threats are limited in the context of the judicious use of available resources.

Concluding, the smart power model highlights and imposes the optimal use of power tools available to a state to achieve national goals, maintaining them in the appropriate level of ambition and supporting the national interest in the long run.

INTELLIGENCE IN TODAY'S SOCIETAL ENVIRONMENT

In the information age (characterised by uncertainty and information abundance – Open Source Revolution, exponential developments of research and analysis in private academia etc.) in which states continue to remain the fundamental factor in organising power and generating order worldwide, the role of intelligence services is mainly to identify threats, through their ability to provide the policy makers with that *"key to decrypting reality"*, represented by the mass of data, facts, events, processes available for the formation of strategic knowledge, which no other source of information can provide (Maior, 2010, p. 31).

The economic-social, technological and institutional challenges of the operational environment to this fundamental activity are amplified in the current context of the SarsCov2 pandemic, with all the limitations, institutional, behavioural, political and social changes related. Without claiming to exhaust all the factors, events or actions with an impact on the proper functioning of state institutions, I present below a recent approach, relatively different from the classic analysis on the PMESIIE model (Political, Military, Economic, Social, Informational, Infrastructure, Environment), which brings to the fore a number of characteristics of contemporary society (developed from another perspective), which intelligence services must take into account.

Thus, the events, phenomena and socio-demographic, technological and informational developments, in a horizon of 20-25 years, could be fundamentally influenced by 10 factors, which would determine the evolution of humanity rather towards the formation of the *"client"* type of individual *(Cliens)* and "angry" *(Iratus)*, than to Homo Deus of whom Youval Harari speaks optimistically in his works (Bondoc, 2020):

1. Secularism (and the secularisation of urban life) has allowed the strong development of science and technology, with related advances, but has focused on material and short-term issues, causing the shift of *"responsibility"* from God to man;

- This situation favours the increase in the number of people with a weaker connection with the divinity, the tendency towards excesses, the weakening of morality, by its descent from the transcendent to the mundane, the increase in popular dissatisfaction, affecting at the same time the feelings of religious people.

2. The development of sewage and drinking water systems, as well as the progress of the pharmaceutical and medical industry have brought immense benefits but have decoupled humanity from natural evolution;
   - Social progress has increased life expectancy, but physically there is dependence on technology and medication, decreased tolerance to pain, discomfort, and increased *"needs"* and expectations of support from outside.
3. Comfort, at home, office and in cities, has led to diminishing challenges and therefore physical and intellectual resistance, for the majority of the population, increasing the gap between life and nature.
   - The degree of difficulty and the number of challenges have decreased for a large part of the population, and the physical consequences (obesity, muscle weakness, skeletal changes etc.) will be complemented by the effects on the human intellect, underused.
4. Permanent stimulation of consumption leads to complex changes in behaviour.
   - Stimulating the frequent multiplication and change (by the appeal of traders mainly to the emotional, mobile side and to prioritising the short term at the expense of reason and the long term) of products and services purchased with a new variant will lead to attenuation of deep relationships and tendency for superficial behaviours, lacking in stable points of reference.
5. The volume and frequency of scientific developments have pushed more and more people towards a feeling of professional and even social inadequacy, as they do not know how to keep up.
   - The current continuous development determines more frequent economic, professional changes and human interactions than a person normally comfortably endures, which generates increased intellectual challenges, the management of which requires external support (guidance or specialised training); many people become resentful and are tempted to politically support populist solutions and offers that, in exchange for votes, promise miracles and blame "others" (the rich, the foreigner, the traitor in the party etc.) for their own difficulties. Constant frustration leads to outbursts of anger.

6. The information society has aggravated the above problems. Although it has greatly facilitated access to information and experiences, it has had serious negative effects.
   - Among them the following can be mentioned: brain flooding with a large volume of data, difficult to manage (feeling overwhelmed), excessive ideas, images, sounds, movements, smells, taste sensations and social interactions being several times higher compared to a century ago; emotional, sensationalist and exhibitionist/tabloid manifestations, to stand out as personal forms of expression (through the media, on social platforms or on other public occasions); the massive spread of false news through the internet (favoured by the natural inclination of the human being towards sensational, conspiratorial news and scenarios, negative towards the normal), which affects the calm and cohesion of society; Immediate *"rewards"*, favouring short-term concentration and dependence on the support of others.
7. Exceeding the level of basic needs, the accumulated wealth and technology of society, as well as the awareness of the vastness and complexity of a global world have induced a sense of security, but also of frustration, with the decrease of individual responsibility.
   - Societal complexity tends to be increasingly difficult to understand, to inhibit individual participation in the general state of well-being, to cover up irregularities and to tolerate the irresponsible (who do not end up being held accountable); politically, the client tends to act in the short term, according to the electoral cycle (4-5 years) or why not, the professional one (to change jobs every few years);
8. Many people have reached to the level in the *"Maslow's pyramid"* at which they want to express themselves and be listened to/appreciated; this coincides with the excessive feeding by marketing and the information society of emotional and positional radicalism.
   - The existence of numerous political, academical, ideological stances determine the appearance and promotion of the radical discourse, so that the message reaches the target; the traditional debate tends to be blurred by this type of discourse and message, which affects the focus on principles, social cohesion and real dialogue.
9. The universal voting system has allowed a reasonable harmonisation of interests between the elites and the general interest for about 70-80 years, but now society is experiencing growing cracks.
   - As long as the socio-economic model sought to cover basic needs, the general interest was harmonised with the real needs of most people,

and the issues under discussion were easier to perceive correctly; due to the overcoming of basic needs in many states, the consumer society in the information age of the wealth of data, products and services pushes to stimulate the emotional and the irrational, with political consequences of favouring emotional debates to the detriment of the rational; there is an urgent need to ensure correct information and democratic training of the population in the first years of school.

10. The phenomenon of globalisation subjects the individual: a. to an intense professional competition; b. to pressure for cultural/identity uniformity too fast; c. to *"upward"* comparisons with the highest (world) standards, including from a socio-political point of view.
    - The human need for security and control determines the tendency of individuals' behaviour towards stability and predictability. However, technological changes have significantly increased the individual and collective efforts for professional and economic adaptation, with the related difficulties and concerns; the tendency for cultural, socio-political and identity uniformity supplements these efforts. The status induced by the permanent client, under the slogan *"the client is always right"* raises expectations in individuals about their rights to others, misunderstood, feelings of frustration, emotional instability, anger, expression of radical messages, negativity, rejection of long-term solutions.

The ten factors have the potential to generate detrimental consequences for human society as a whole:

- The physical and mental decline of the average person, although there are many premises for significant progress.
- The emergence of a new type of *"religion"*, consumerist, exaggerated, premature and unsustainable, for large segments of the population, which are disconnected from their own contribution to society.
- The temptation, from more and more groups of individuals of communicative aggression of those who have a different opinion, including the destruction of current social models, without proposals for replacement, which becomes similar to an anarchic approach.
- A tendency of cheerful irresponsibility manifested by many decision-makers, on different levels of exercising public functions, with prospects of aggravation of problems.

The highlighted factors feed into each other and encourage deviant behaviours, which must be counterbalanced by the right mix of smart and reasonable public policies, with a special note on preparing the younger generation to properly manage the abundance of information to which it is subjected.

With regard to intelligence, the policies need to take into account that relevant societal change drivers are pushing intelligence services to experience a paradigm shift, which is generally in the form of transition processes specific to change management, based on a series of axioms (Nițu, 2018, p. 218):

- from classical, symmetrical and clear risks to asymmetrical, increasingly diffuse and non-linear risks;
- from information to intelligence;
- from state-focused security to individual security (human security);
- from intelligence agencies to (increasingly integrated) intelligence communities;
- from competition to cooperation and synergistic work between agencies through joint task forces on clear and specific objectives, areas or topics;
- from national security systems to joint undertakings by objectives, areas or topics of expertise;
- from the linear intell cycle to network intell processes;
- from information resources management to knowledge management;
- from old to new IT applications;
- from need to know to need to share and even responsibility to provide;
- from the division of labour to multidisciplinary task forces and fusion centres;
- from the focus on forecasts to scenarios and simulations designed to change the future;
- from in-house training methods to extensive partnerships with academia and civil society;
- from paper-based intell products to briefers that interact directly with consumers/beneficiaries.

The process of change is directly focused on the staff training and education processes in institutions responsible for managing information resources and knowledge, causing decision-makers and leaders of education and training structures to formulate and materialise new formulas for strategic innovation and transformational decisions (Colesniuc, 2019).

PERSONNEL AND STAFF TRAINING – STRATEGIC FUNCTION OF INTELLIGENCE INSTITUTIONS

The intelligence services are part of the same logic of operations in any organisation (defined, controlled and coordinated form of human activities to achieve the proposed goals), regardless of their functional orientation, in the constitutive manner: profit – non-profit/state – private.

The components of any organisation, including those working in the field of intelligence, are primarily dependent on the human factor, its quality, motivation, employment, satisfaction, leadership and interaction in a regulated framework and oriented to a previously defined purpose.

The *smart power* model for intelligence services cannot be developed on an educational component without appealing to the historical and institutional continuum. Strategic knowledge is generated and becomes more developed by assuming the legacy of previous knowledge, institutional experiences, transformed into lessons learned, which are included in the current educational process for training experts and leaders. The curricula design has to take into account both the beneficiaries' training request, expressed and transposed in the graduate model or the competencies aimed to be achieved at the end of the training (from the perspective of being, knowing, doing), as well as the evolution of the security environment in the fundamental fields (political, economic-financial, socio-cultural, military, technological, infrastructure, environment and climate) whose understanding and knowledge is conferred by the cognitive-interpretive functions of the training structures.

The whole vocational training process includes at least three important participants, who thus build a mutually beneficial relationship: the *"student/employee"*, the *"instructor/professor"* and the *"beneficiary/employer"*.

Their interaction is under the obligation to define, adopt, internalise and develop those professional skills, values, attitudes and behaviours for the benefit of the product of educational and training process (the student) to be able to contribute to the mission of the organisation, the intelligence service. This is minimally defined as avoiding strategic surprise and providing current information and strategic knowledge for decision-makers, and, in the future, to promote the continuous improvement of internal processes to ensure the performance of the institution and its adaptation to current and future security challenges.

Analyses on the skills required by the labour market in populated urban areas, larger than 100,000 inhabitants, show the preference, the tendency of companies to hire staff, on the distribution of soft (a) and hard (b) skills, respectively, which prove or hold: a. creativity (similar to 2019), persuasion (s.2019), ability to collaborate (s.2019), ability to adapt (s.2019), emotional intelligence; b. competencies regarding: blockchain, cloud computing, analytical reasoning (s.2019), artificial intelligence, UX Design (s.2019), business analysis, affiliate marketing, sales (s.2019), scientific computing, video production (Pate, 2020).

One of the important and constant objectives of the organisations involved in the education and training process is the training of leaders. Declaratively, it is a permanent topic evoked by the management of any organisation, whether it is a public institution, company or non-governmental organisation. Intelligence services are no exception. The challenge of the process itself, with tactical characteristics, at first sight, has strategic influences, as it represents the option for continuity and performance of the current leadership, which must be subsumed under the triangulation of ethos-pathos-logos.

Therefore, in the curricula design, the issues of concern are legitimately expressed regarding: the optimal weight of the specific disciplines; the centre of gravity of this training; defining the relationships and limits between technical, social, communication and leadership skills; the adequacy of the technical-scientific tendencies to the formation of competencies; the influences of the operational environment on the training requirements; managing the pressure exerted by the exponential evolution of the IT&C domain on staff training.

As an example, at least five technological developments will significantly transform the information-operational environment specific to intelligence structures, with implications on the process of designing training and education for personnel, appropriate to them (Vasian, Iorga, 2019, p. 82):

1. Extensive dependence on the Internet of states, organisations and non-state actors, globally, by exploding connections and increasing the speed of access to network services (4G/5G), of human users, both in economic and social areas strongly developed and in poorly developed regions generating insecurity – diminishing human interaction and migration to digital human interaction;
2. Defining and manifesting the cyber environment, with all its components (hardware, software, management, personnel), as a new military operational environment, relevance also recognised by NATO – new offensive action capabilities on the border between conventional and hybrid;
3. The emergence and widespread implementation of global smart surveillance systems in the Internet environment (including DarkNet), in digital communications networks (mobile, fixed, terrestrial, satellite etc.) and in civil monitoring systems and security – advanced technology for algorithmisation and automation of operational intelligence processes;
4. Accelerated implementation of artificial intelligence (AI) algorithms in IT services, weapons and security systems, industry and society, while developing application-type AI tools (machine learning, Natural Language Processing – NLP and Computer Vision), able to successfully replace the human factor – robotisation and algorithmisation of intelligence domains such as OSINT, CYBERINT, HUMINT, IMINT, GEOINT.
5. Achieving technological maturity and increasing the relevance of industry and space technology, while facilitating access to these developments

for non-state actors and less developed states, but aiming at the rapid acquisition of high-tech tools usable both in power relations and in achieving defensive and offensive security purposes – moving military confrontations in the space field, technologization of surveillance tools and ISR-type systems.

These developments, a direct result of the application of advanced technology in civil society and the military in the past 10 years, will be the main factor in reshaping the operational and information environment for the interest of any intelligence structure, regardless of region, area or field. The technological aspects mentioned above will require the separation of the current training processes on two or even three levels, as follows: the training stage, the advanced education stage and the development stage of the strategic culture on security, intelligence and technology (Ibid., p. 89).

Nevertheless, these approaches address a category of adults, which requires the use of the andragogical model (different from the pedagogical model), whose functionality and efficiency are based on a number of principles that take into account: the respect of didactic staff for the audience; institutional collaboration between educator and educated persons, mutually advantageous (involvement of the beneficiary in the development of training planning documents and of the trainees in the evaluation of the training process); the independence designed for students to facilitate achieving their decision-making autonomy; the professional and life experience of the students (through which they can contribute to and offer suggestions and proposals for improving the contents of vocational training; facilitating participatory training methods etc.), solving problems (problematisation and development of content as close as possible to reality, which imposed appropriate solutions); critical thinking (Dragoman, 2017, pp. 73-82).

As a defining element for the function of adapting the organisation to the operational environment, the training and continuous professional education of staff in intelligence services thus becomes an activity with a strategic, institutionalised dimension, which ensures and fully covers the need for continuity and progress of the institution, as a functional system intended for the welfare of society.

CONCLUSIONS

Conceptually, but also in action, the smart power model requires the decision-makers to choose those power tools that correspond and respond best to managing the challenges to a state's interests.

The adequate and optimised use of the available means and resources requires decision-makers to benefit from a strategic knowledge (considered both in depth and horizontal and prospective openness) that can only be provided by national intelligence services, institutionally, through interinstitutional cooperation formats, departmental, but also at international level through bilateral cooperation or security cooperation formats.

Under the pressure of the information society and the open-source revolution, intelligence services are experiencing a paradigm shift, necessary to adapt to the constantly evolving characteristics of the operational environment.

As a component part of the institution, the structure of education and training, which fulfils a strategic function, must meet the requirements of the beneficiaries, regarding the definition, implementation and training of professional competencies, and, at the same time, can contribute prospectively and formatively with evaluations, solutions and proposals for the continuous modernisation and alignment of specific education and training to the characteristics of today and future society.

BIBLIOGRAPHY:

1. Bondoc, L. (2020). *Homo Cliens şi Homo Iratus*, www.contributors.ro/homo-cliens-si-homo-iratus/, retrieved on 5 October 2020.
2. Colesniuc, D (2019). *Educația de intelligence, inovare strategică*, *"Gândirea Militară Românească"* International Conference Proceedings, București.
3. Idem. (2019). *Centrul de pregătire în domeniul informații pentru apărare – adaptare trasformațională a proceselor de instruire și educație în dinamica mediului de securitate*, in Infosfera no.2/2019.
4. Dragoman, M.M. (2019). *Andragogia şi metodele moderne în educarea ofiţerilor de informaţii în învăţământul de formare profesională continuă* in Infosfera no.2/2017.
5. Maior, G.C. (coordinator, 2010): *Cunoaşterea strategică în era globalizării in Un război al minţii – Intelligence, servicii de informaţii şi cunoaştere strategică în secolul XXI*, Editua Rao, Bucureşti.
6. Medar, S.T (coordinator, 2007): *Capabilităţi ale serviciilor moderne de informaţii*.
7. Mocanu, M. (2018): *O teorie generală privind conceptul elementar de risc*, Editura Universităţii Naţionale de Apărare *"Carol I"*, Bucureşti.
8. Mocanu, M. (2018): *Analiza strategică în mediul de securitate contemporan*, Editura Universităţii Naţionale de Apărare *"Carol I"*, Bucureşti.
9. Niţu, I. (2018): *Analiza de intelligence – O abordare din perspective teoriilor schimbării*, Editura Rao, Bucureşti.
10. Nye, J.S.Jr. (2002): *The Paradox of American Power. Why the World's Only Superpower Can't Go It Alone*. Oxford University Press.
11. Savu, G; Pârlog, A. (2009): *Producţia de intelligence*, Editura Medro, Bucureşti.
12. Vasian, B., Iorga, B. (2019): *Evoluţia structurilor de intelligence în era tehnologiilor avansate*, in Infosfera, Bucureşti, no. 4/2019.
13. The Top Skills Companies Need Most in 2020 – And How to Learn Them, www.linkedln.com/business/learning/blog/top-skills-and-courses/the-skills-companies-need-most-in-2020and-how-to-learn-them, retrieved on 2 October 2020.
14. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf, retrieved on 14 September 2020.

THE USA AND *SMART POWER* POLICY

Vasile SANDOR

Theoretical High School "Ştefan Odobleja", Bucharest

In the circumstances in which the image and the influence of the USA deteriorated all over the world at the beginning of the 2000s, The Center for Strategic and International Studies (CSIS) of the USA founded a Bipartisan Commission for Smart-Power, with the purpose of drawing a vision which will develop a set of rules on the basis of which the next president of the USA, regardless of his political view, can implement smart-power policy.

Among the arguments that served as a basis for establishing such commission were the opinion polls that indicated the deterioration of the USA image all over the world. President George W. Bush was perceived as a threat for the world through comparison with the President of Iran Mahmoud Ahmadinejad, and the one of North Korea Kim Jong Il.

In that context, the Commission reckoned that the American leaders had to promote a positive political vision, more powerful than the war against terrorism.

Keywords: war; influence; positive vision; smart power; public diplomacy;

INTRODUCTION. HARD POWER/SOFT POWER/SMART POWER

The concept of *smart power* was introduced at the end of the 80s by Joseph Nye Jr., former Deputy Secretary of Defense during the Clinton administration, in antithesis to *hard power*, which consists of the use of force and procurement in order to meet the goals. Moreover, the concept is deemed as *"the second face of power"* (Bachrach, Baratz, 1962, pp. 947-952), which allows the indirect achievement of the desired political objectives and not only, by means of: culture – appreciated and accepted beyond frontiers –, political values, implicitly positive and superior, practiced inside and outside the state, and foreign policy, when it is perceived as legitimate and moral.

Soft power derives from values, culture, institutions, and behaviour that emanate both from society and from the government. The United States of America accumulated soft power during the 20*th* century due to the fact that they acted according to their founding democratic ideals; they displayed their values through programmes such as the Marshall Plan; they propagated an attractive culture and lifestyle, both by means of governmental programmes and the media, such as *The Voice of America* and *Radio Liberty*. The US soft power was strategically the most powerful in Japan and Europe, although the phenomenon was global.

Starting in 1953 until its unification with the Department of State, the US Information Agency – USIA coordinated most part of the US public diplomacy and developed the *soft power*. Although it was not perfect, the Agency achieved a credible performance by telling the world the story of America through its cultural, educational and informational programmes. The Agency, having more stations in the world than any other governmental agency, unfolded the greatest operation of public policies compared to any other nation, being also the greatest editor and a formidable broadcaster of radio shows. However, a recent analysis made by Nicholas Cull (2006) highlights the contrast between the performance during the Gulf War (1991) and the failures at the beginning of the 2000s (Ibid., vol. 15). The decline started during the first years of the 1990s, when the North American executive and legislative branches decided that the financing level of the public policies was (no longer) necessary, and consequently the USIA went through major cuts and even a kind of marginalisation. The function of broadcasting was integrated into a system of non-military broadcasters of the American government, and the function of public policies did not do very well within the framework of the traditionalist State Department for Culture.

THE DECLINE OF US IMAGE OVERSEAS

A great number of studies carried out in the first years of the 2000s revealed that the public policies for integration manifested planning and strategic coordination deficiencies at the government level, within the Department of State and between the States and the embassies. The most serious problem remained the inadequacy of the personnel and the resource programme intended to sustain a minimum mobilisation in the world. The Congress used to allocate approximately 630 million dollars to the Department of State for public policies, and approximately 645 million dollars for civil broadcasting, a total of 4% of the expenditure budget for international problem and 0.6% of the Pentagon budget (An American Budget, 2018). All this in the context in which the USA spent for public policies as much as Great Britain and France, despite the fact that the USA is five times larger than these two states, and had much more serious credibility problems. If the USA had spent with the Muslim world as much as it did with Germany and Japan during the post-war period, the budget should have had to amount to 7 billion dollars (Smith, 2007).

For the USA, *smart power* is a combination between *hard power*, which entails the development of an integrated strategy, resources, and a set of tools to achieve the objectives. It is an approach that highlights the necessity for strong armed forces as well as massive investments in alliances, partnerships and institutions at all levels, so as to extend the US influence and to legitimise the American actions. The delivery of betterment in the entire world is the main goal of this effort, because that helped the USA to reconcile their overwhelming power with the interests and values of the rest of the world.

However, there were three major obstacles. The foreign policy of the USA tended to overbid hard power, as it was more direct and because smart power entails the development of an integrated strategy. The Pentagon is the best prepared structure and has the largest resources within the framework of the federal government. As a result, it tends to occupy any gaps that the public institutions should have filled. The USA must maintain its military superiority but in the current climate there are limitations to what hard power can obtain on its own.

The foreign policy of the USA wants to develop *soft power* instruments. More often than not diplomatic instruments and foreign assistance are directed toward states that compete for power within their borders with non-state actors. Diplomacy and foreign assistance are underfunded and underused many times. These tools are neglected, partly because of the difficulty of demonstrating their short-term impact in the case of critical challenges.

The foreign policies of the USA are fractured and chambered. Coordination, where applicable, occurs at the relatively inferior level, or others of them are at a very high level of administration, both making impossible the long-term planning during crises (CSIS, 2017).

The situation of the USA foreign policy changed during the time Karen Hughes occupied the position of Under Secretary of State for Public Diplomacy and Public Affairs but then the position was vacant for almost half of the first term of the President George W. Bush administration. After one year in office, Hughes developed more specific changes, with a view to applying the smart power policy. Between 2002 and 2006, the funding of the programmes of educational and cultural changes increased by 25% in the Middle East, and by 39% in Southern Asia, whereas the financing of the public policy increased by 21%, despite the fact that the number of the officers remained unchanged. 21 rapid response units were established in Brussels and Dubai, the latter having a public diplomacy officer that could fluently spoke Arabic and who appeared regularly on Al-Jazeera and other channels of the Middle East Television. Then, the ambassadors were able to publicly advocate the USA policies directly in the press, contrary to the previous press-wary rules. The US government invited American Muslims, business persons and cultural personalities to take active part in the spreading the US message worldwide. Hughes established a coordination mechanism of the public diplomacy within the government, especially between the Department of State and the Department of Defense. Many officers were trained in public diplomacy skills, the relevant heads of the public diplomacy being able to become part of the structures of political decision-making.

Although Hughes were assailed for her lack of skill in the international issues, her campaign style approach, her focus on projects instead of strategies, and the implementation of those changes reinvigorated the public diplomacy. Due to Karen Hughes' activity, the US message to the world improved.

Much of the world, nowadays, has a negative opinion of the USA, regarding it as dangerous and unpredictable. Recent worldwide surveys have confirmed the continuous deterioration of the US image in the global public opinion, this trend being deepened after the US presidential elections in 2000, and it suddenly accelerated in 2003, after the invasion of Iraq by the Americans and their allies.

SMART POWER AND THE RESTORATION OF THE US IMAGE OVERSEAS

The current attempts to edify a support for the US policy and the American values, from the global public diplomacy of the Department of State to the public affairs of the Department of Defense in war areas, have failed, as well as the attempts to reverse the negative anti-American attitudes that were so severe that antagonised the US ability to achieve their foreign policy goals. The anti-American forces have obtained an advantage attributed to the downfall of the USA popularity around the world, turning the anti-Americanism into a threat to their security.

The US government should have taken the necessary measures immediately and quickly in order to regain their credibility in the entire world. President Bush administration should have revised a part of its policies and should have moderated the style of the international discourse, so as to regain the favour obtained by the USA previously.

It was crucial to put much more emphasis on public diplomacy. In addition, the Congress and the executive branch should have used the next two years to restructure the soft power instruments of the administrative apparatus, making them more effective and powerful (Smith, Ibid.).

America obtained low scoring in polls. Pew Research Center demonstrated in 2006 what the polls of the previous years had shown: the global public opinion had firmly turned against the USA. The favourable attitude to them had deteriorated in almost all the polled countries in Europe, Asia, and especially the Middle Est. The USA had never been so unpopular in the Western Europe. Even in the UK, 41% of those questioned were of the opinion that the USA were a greater menace to the world peace than Iraq was (The Guardian, 2006).

In 2008, Andrew Kohut and Richard Wilke, the manager and the associate manager of the Institute of Pew Global Attitudes Project, summarised the findings of the Institute on the decline of the USA image between 2002-2007, following a comprehensive research – All the world is a stage. Their conclusions, simply put, were as follows: the USA image in most part of the Islamic world remained abysmal. Pew applied questionnaires in 47 countries. In 9 countries, less than 30% of population had a positive opinion of the USA. Turkey had the lowest opinion with 9%, then the Palestinian Territories with 13%, Pakistan and Morocco with 15%, Argentina with 16%, Jordan with 20%, Egypt with 21%, Malaysia with 27% and Indonesia with 27%.

At the same time, the study revealed that the support of terrorism had dropped dramatically in many Islamic states, and that fewer Muslims considered the bomb suicide justifiable, and the trust in Osama bin Laden had decreased as well (IPDGC). Moreover, the majority of the questioned countries regarded China more favourably than the USA. In Turkey, a country that is a NATO ally, only 12% of those questioned had a favourable opinion of the USA, in comparison to 52% in 2000. In Indonesia, the favourable attitude decreased from 75% in 2000 to 15% in 2003, subsequently increasing again in 2006 to 30% (Ibid.).

A survey ordered by the newspapers in Canada, Great Britain and Mexico in 2006 revealed the fact that President George W. Bush was perceived as a threat to the world, in comparison with the President of Iraq, Mahmoud Ahmadinejad, the President of North Korea, Kim Jong Il, and the Hezbollah leader, Hassan Nasrallah.

The favourability with the Americans in 2005 dropped in nine of the surveyed countries. According to a momentous statement of the journalist Roger Cohen from the New York Times, the world *"has stopped buying the American story"*.

A list of supplementary complaints completes the image. The public opinion accused the George W. Bush administration of unilateralism and preemption, due to the firm support for the state of Israel and the disdain shown to the international organisations. The decision of the Bush administration to leave the Kyoto Protocol and to deny the threat of global warming were met with consternation by the most important Asian states and the European allies, giving birth to an additional irritation.

The goodwill reserves accumulated during the previous decades vanished, as well as the global popularity felt for the USA immediately after 11 September 2001. Many Americans agree that the anti-American feelings historically occur in cycles and they are a part of the burden carried by any great power. Sometimes the antipathy toward the USA contradicts their optimism, and it is very unlikely to decrease without taking energetic correction measures.

The final report of the Princeton Project on the National Security, made by G. John Ikenberry and Anne-Marie Slaughter, (*Forging a World of Liberty Under Law: US National Security in the 21st Century*, 2006), offers a strategy cut out for a world which lacks the principles of a unique organisation, as the anti-fascism and anti-communism. The findings are guided by six criteria: the implementation of different instruments in different situations, according to the current findings, the combination of hard power with soft power, frameworks of cooperation based rather on interest and hope than fear, the consolidation of capacity, integrity and internal accountability of other governments, and the adjustment to a world *"in which information travel instantaneously, the actors also answer it instantaneously, and small specialised units reunite for purposes defined for a limited period"* (Ikenberry, 2006).

In the winter/spring issue of *Georgetown Journal of International Affairs*, the former US ambassador in the Republic of Moldova, Pamela Hyde Smith, stated that the approaches at that time regarding the support of the US policy and the American values abroad did not succeed in reversing the negative attitudes toward the North-American State, this assertion being confirmed by the opinion surveys, whose results were published by Globe Scan and the Program of the University of Maryland on the international political attitudes on 23 January 2007, which proved the ambassador's observations.

The image of America abroad – with very few exceptions – continues its evolution in downward spiral. And, as ambassador Smith signals, *"the anti-American* *forces take advantage of the drop in the US popularity worldwide, turning the anti-Americanism into a threat to the national security"* (Smith, Ibid.). The five-page Manifest of the organisation Revolutionary Fight (E.A.) – a Greek terrorist group, which took responsibility for a missile attack over the American Embassy in Athens on 12 January 2007 -, is the most recent confirmation of its sombre evaluation.

The foreign policy of a state exerts the most power influence; few foreign societies will approve the US policy, in case they believe they put in jeopardy their own interests. For instance, in the Islamic world, the US war against terrorism is perceived as being directed against the Islam, thus exacerbating the anti-western accents of the Islamic fundamentalism (Ibid.).

Ikenberry and Slaughter supplied a prospective analysis on the threats and opportunities of the 21st century, governing, soft power, public diplomacy, information technologies and the implications of information affluence (Ibid., 2006). The two above highlighted the necessity of an infrastructure that allows the officials of national security to play chess at the same table and at the same time with two state and non-state actors, in a time that runs fast and with rapid changes of rules. Instead of creating a new bureaucracy, they state that the USA must (inter) connect the existent ones. Instead of creating command structures vertically, they must construct horizontal networks and direct them from the centre, rather than direct them from top to bottom, or the other way round. Instead of building all the new governing capacities, the USA must learn to exploit the capacities of the internal and external private actors (IPDGC, Ibid.).

Considering that the US image and influence deteriorated all over the world at the beginning of the 2000s, the Center for Strategic and International Studies (CSIC) of the USA established in 2006 a Bipartisan Commission for Smart Power, with a view to developing a vision that should direct the US global commitments as well as a set of rules based on which the next president of USA, regardless his/her political orientation, can implement the smart power policy.

Among the premises underlying the activity of this Commission, there were opinion surveys that pointed to the worldwide deterioration of the US image and the American people: Pew Global Attitudes Project in 2006, Zogby survey, World Public Opinion survey in 2007, the survey of BBC World Service in January 2007 etc.

The Commission appreciated that in the elections of 2008 an important subject was to be the issue of ensuring a higher degree of security for the American citizens, under the circumstances of the danger presented by the global menace of terrorism and violent extremism. The US commitment in the fight against this peril, in the Commission opinion, must have been made based on four principles: the US leaders should have been on the offense against international terrorism, but they should have avoided answering to provocations in an exaggerated manner; they should have also needed to eliminate the symbols of an intolerant, abusive, and unjust America; the use of diplomacy for positive finalities; the American leaders should have promoted a positive vision, stronger than the war against terrorism. The Americans needed an important goal to strive for, not only a simple tactic.

This problem of *smart power* policy was in the centre of attention of the Institute for Public Diplomacy and Global Communication from *"George Washington"* University. Within Landon Lecture (2007), there was raised the issue of strengthening the US capacity of using soft power and a better integration of it into hard power. The recommendations included the increase in the national capacity of economic growth, edification of institutions, law enforcement, good governance and strategic communication; a better use of expertise in the American universities; a dramatic increase in the expenditure for civil instruments of national security – diplomacy, strategic communication, external assistance, civil action and reconstruction and economic development. The path of institutionalising these capabilities is, most probably, not the recreation or the popularisation of the institutions of the past, such as USIA. The USA needs to ponder on the methods of integrating the government capabilities into those in the private sector, from universities, NGOs, with their allies and friends (IPDGC, Ibid.).

The American strategy for strategic communication and public diplomacy also established the categories of the target audience. They are represented by opinion makers from different countries – clergy, teachers, journalists, leaders, scientists, military and political personalities –, so-called vulnerable segments of population – including here youth, women and minorities –, and mass audience. The priorities of public diplomacy, to make the achievement of the objectives entrusted to it possible, are given by the extension of educational programmes and cultural exchanges, modernisation of communication means, promotion of fact diplomacy. As a conclusion of the document, it is stated that public diplomacy is a promoter of peace that pursuits the fulfilment of the conditions that ensure that all people in the world can have a better life, and that extremism cannot spread (Şerban, 2011, p. 81).

In October 2007, Tom Miller published *America's Role in the World: A Business Perspective on Public Diplomacy*, a report in which the public diplomacy definitions were analysed, debating the problems of the American economy led by the decline of the US public image, and recommending methods that could be used by the community of businessmen to help with the restructuring and promotion of a strategy of effective public diplomacy. The Business for Diplomatic Action (BDA) recommendations were: creation of a corporation of independent public diplomacy and an agency, the National Council for Communication, which reports (only) to the President, development of a public diplomacy and a communication strategy that employ aptitudes, techniques and processes of global businesses, an increase of the resources allocated to them, from 1.5 billion dollars to 3 billion dollars, the establishment of a Body of Reserve Officers of the Foreign Service and Goodwill Ambassador (IPDGC, Ibid.).

Richard L. Armitage, former deputy of the Secretary of State, Joseph S. Nye, Jr., co-presidents of the Commission for smart power, CSIS (2007), and a bipartisan commission of scientists and practitioners, request the US president to implement a smart power strategy complementary to the economic and military power, with great investments in soft power. They recommended the focus on six areas: reinvigorated alliances, partnerships and institutions, high global development, reinforced public diplomacy, economic integration, technology and innovation, creative approach of the arrangement of the organised, coordinated, and budgetary governance. The recommendations regarding the public diplomacy included the raise of exchanges (of students, scientists etc.), focused on youth, educational funds of USA - China and USA - India, linguistic competences for extended Middle East, and the creation of a non-profit centre for international knowledge and communication (Ibid.).

David Boren, the president of Columbia University, former democrat senator and chairman of the Committee for the Senate Information, in his book *A Letter to America* (2008), takes a balance look at the US political system that is increasing in cynicism, as well as the reforms necessary to the internal and external policies. The following are among Boren's priorities: a better understanding by the Americans of others' culture and history, the increase of the students and scientists flow to and from the USA, from the countries important for their future, relaxation of the conditions of awarding the visa for students, an International Peace Corps shaped after the model of the similar American Institution, and the creation of a *"reserve government of independent thinking"* in order to allow the scientists, the business leaders and the journalists with global experience to share their expertise and way of thinking, without compromising their independence (Ibid.).

James Glassman, in the *Public Diplomacy in the 21st Century*, (2008), during his first speech given as the Under Secretary of State for Public Diplomacy and Public Affairs, former chairman of the Board of Radiobroadcasting Governors, commented on the instruments and plans of the traditional public diplomacy, his approach on public diplomacy defined as a *"a war of ideas"* that is concentrated on *"winning the war against terror"*. He appreciated that the US radiobroadcasting was extremely efficient, and the Department of State being a *"jewel of the public diplomacy crown"*. He understood that his role as the Under Secretary of State was *"to perform his part of public diplomacy ... which goes to the USA"* and *"to make a comprehensive governmental effort within the war of ideas"*. He considered that the US public diplomacy had *"to tell the world about a good and merciful nation and to engage in the most important ideological competition of the present – a competition that we (the USA) will win"* (Glassman, 2008). What was his opinion of reaching this goal? By using the tools of the ideological commitment – words, facts, images –, in order to create a hostile environment for violent extremism.

The ambassador Michael C. Polt, with a career in the US Foreign Service achieved during the application of Marshall Plan in Germany, offered in 2008, six recommendations for the next president: restructuration of the embassies all around the world, treating of the US diplomacy as a serious profession, reassertion of the role of the diplomatic corps as the main agent to meet the objectives of the President foreign policy agenda, creation of a single, substantial and consistent budget of foreign policy for all the US efforts abroad, creation of regional councils of ambassadors and putting the trust in professional diplomats (Toolbox, 2008).

In the report of the Consultative Commission for Public Diplomacy, entitled *Getting the People Part Right: A Report on the Human Resources Dimension of U.S. Public Diplomacy* (2008), the above-mentioned Bipartisan Presidential Commission appreciated critically and in detail the personnel recruitment, training, evaluation, structures and the integration of the public diplomacy officers into the Department of State nine years after its unification with the US Agency of Intelligence. Among his main conclusions: the states do not make any special efforts to recruit public diplomacy officers with relevant experience or skills; within the analysis of the Foreign Service, tests are not performed to identify predilections or skills for public diplomacy; the training of public diplomacy is sound, but there are many blind spots; the State's Foreign Service Institute must develop courses at a level comparable with the license university courses, and must establish serious nine-month courses from medium to superior level; State's evaluation process overwhelmingly rewards public diplomacy management rather than outreach; the state must undertake a comprehensive revision of the public diplomacy structures from the geographic offices and missions all around the world; the persistence of under-representation of the public diplomacy officers of superior rank was emblematic in furthering the lack of progress of the public integration into the basic work of the Department of State (IPDGC, Ibid.).

CONCLUSIONS

In a world that has rapidly become multipolar, with new emergent states, with power skills that are at least regional, the time has come to adopt a new perspective vision of the American power. More than ever, in such circumstances, the USA must rethink its strategies, and the *smart power* is inevitably necessary to become an essential component of these strategies.

According to Joseph Nye, the USA must not give way to panic, under the circumstances of its decline and the increase of China's power. The US decline is appreciated as relative and it is likely that the USA will remain more powerful than any other states during the coming decades.

The yesterday promoter of soft power, Nye pleads for the new strategic concept of smart power. Established on the ability to influence and form alliances, the new stand is tailored according to an America that is mourning for hegemony, but by no means renouncing to leading the world.

Joseph Nye considers that the USA must not surrender to the fear of decline or the temptation of withdrawal but rather it must define its role in a more interdependent and complex world than ever. The problem of the American power in the 21st century is not that of decline but the rise of a new question: what must be done when it becomes obvious that not even the most powerful state can reach its goals without the support of the other states? The answer takes shape under the form of a strategy called *smart power* that is based on a new vision of power, in which power makes room for collaboration. A growing number of challenges will force the USA to exercise its power rather together with other states than use it upon them.

More specifically, this fact entails not focusing only on the hard power especially belonging to the military forces, but also resisting the temptation of unilateralism or maintenance of hegemony that characterised the time of President George W. Bush, preferring to form alliances and networks, from the perspective of what the companies are already doing. Smart power does not consist of power maximisation or hegemony maintenance, but it entails the combination of the means available within the strategies adjusted to the new context of power diffusion and the emergence of new powers. In other words, it is about mourning hegemony in order to play better the leading game, with intelligence and subtlety (Smart Power, 2010).

BIBLIOGRAPHY:

1. Bachrach, P., Baratz, M. (1962). *"Two Faces of Power"*. In The American Political Science Review. Vol. 56, no. 4.
2. Boren, D. (2008). *A Letter to America*. University of Oklahoma Press.
3. Cull, N. (2006). *US Public Diplomacy and International Broadcasting During Desert Shield and Desert Storm, 1990-1991*. Transnational Broadcasting Studies Journal. Vol. 15.
4. Glassman, J.K. (2008). *Public Diplomacy in the 21st Century*. Washington, D.C., http://www.cfr.org/publication/16698/public_diplomacy_in_the_twentyfirst_century_rush_transcript_federal_news_service.html, retrieved on 24 September 2020.

5. Ikenberry, J.G., Slaughter, A.-M. (2006). *Forging a World of Liberty under Law: U.S. National Security in the 21st Century*. Princeton University: The Woodrow Wilson School of Public and International Affairs.
6. Kohut, A., Wilke, R. (2008). *All the world is a stage*. In *The National Interest*.
7. Miller, T. (2007). *America's Role in the World: A Business Perspective on Public Diplomacy*. Business for Diplomatic Action (BDA).
8. Nye Jr., J.S. (2010). *The Future of American Power*. In Foreign Affairs.
9. Smith, P.H. (2007). *The Hard Road Back to Soft Power*, https://ciaotest.cc.columbia.edu/olj/gjia/8_1_winter_spring_2007/8_1_winter_spring_2007_c.pdf, retrieved on 11 September 2020.
10. Şerban, I.D. (2011). *Diplomaţia publică – instrument politic pentru SUA ca smart power. Analiză cauzală*, Ileana%20Daniela%20%C8%98ERBAN%20-%20DIPLOMATIA%20PUBLICA-%20INSTRUMENT%20POLITIC%20PENTRU%20SUA%20CA%20SMART%20POWER%20-ANALIZA%20CAUZALA.pdf, retrieved on 23 September 2020.
11. *An American Budget* (2018), https://www.whitehouse.gov/wp-content/uploads/2018/02/budget-fy2019.pdf, retrieved on 11 September 2020.
12. CSIS/Commission on Smart Power. (2007). *A smarter, more secure America*/co-chairs, Armitage, R.L., Nye, Jr., J.S.
13. Getting the People Part Right (2008). *A Report on the Human Resources Dimension of U.S. Public Diplomacy*.
14. IPDGC. (2018). The George Washington University, https://ipdgc.gwu.edu/author/yvonneoh/page/18/, retrieved on 12 October 2020.
15. *Remarks as Delivered by Secretary of Defense Robert M. Gates*. (2007). Landon Lecture (Kansas State University) Manhattan.
16. *Smart power: comment les États-Unis préparent la fin de leur hégémonie*. (2010). In Grenoble École de Management. Comprendre les Jeux Politiques. Note Hebdomadaire d'analyse géopolitique.
17. *Toolbox: Strengthening American Diplomacy*. (2008). The American Interest. Vol. III.
18. *US seen as a bigger threat to peace than Iran, worldwide poll suggests*, https://www.theguardian.com/world/2006/jun/15/usa.iran, retrieved on 12 October 2020.
19. https://www.csis.org/events/csis-commission-smart-power-report-release-event, retrieved on 12 October 2020.
20. https://go.gale.com/ps/anonymous?id=GALE%7CA160281243&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=15260054&p=AONE&sw=w, retrieved on 23 September 2020.
21. https://ipdgc.gwu.edu/author/yvonneoh/page/18/, retrieved on 3 October 2020.
22. https://ciaotest.cc.columbia.edu/olj/gjia/8_1_winter_spring_2007/8_1_winter_spring_2007_c.pdf, retrieved on 3 October 2020.
23. https://ipdgc.gwu.edu/author/yvonneoh/page/18/, retrieved on 11 September 2020.

GLOBAL AGENDA *"WOMEN, PEACE AND SECURITY"*: MAINSTREAMING GENDER PERSPECTIVE IN THE SECURITY SECTOR OF THE REPUBLIC OF MOLDOVA

Assoc. Prof. Natalia ALBU, PhD
"Alexandru cel Bun" Military Academy, Chișinău
Scientific Researcher and Coordinator,
Institute of Legal, Political and Sociological Research, Chișinău

During 2000, the UN SC launched an intense discussion on protecting the rights of women in conflict situations and increasing their role in the peacemaking process. Regardless of the cultural level and that of mentality, wars and armed conflicts affect in a similar way women's condition. On 31 October 2000, the UN SC adopted unanimously the Resolution 1325 on Women, Peace and Security, being one of the most important UN resolutions in the area of peace and security, and being mandatory for all the UN Member States, without the need to be additionally ratified. Currently, the principles and values promoted by the UNSCR 1325 serve as basis for the fundamental values of EU, NATO, OSCE, EC.

The international commitments assumed by the Republic of Moldova Government in implementing the UN SC Resolution 1325 on Women, Peace and Security, as well as the problems identified at the national level in relation to ensuring an inclusive security sector have determined the need to develop and approve a National Action Programme. Although the Women, Peace and Security Agenda is a relatively new topic for the Republic of Moldova, there are already some lessons learned, such as: (1) the need to encourage the decision-makers to foster the political will for implementing the UNSCR 1325, (2) the need to ensure an inclusive security sector and (3) the lack of resources dedicated to implementing the UNSCR 1325.

The discussions regarding the implementation of the UNSCR 1325 is one of considerable importance in the context of the global crisis as a result of the COVID-19 pandemic. Undertaking immediate measures to counteract the threats induced by COVID-19, the states neglect the implementation of the UNSCR 1325. But the states acknowledge less the fact that the coronavirus pandemic invites to collaboration based on the principles established in the UNSCR 1325, taking into account the different security needs regardless of COVID-19 or any other threat.

Keywords: Resolution 1325; Women, Peace and Security Agenda; Action Plan; security needs; female leadership; COVID-19;

INTRODUCTION

In 2020, it has been 20 years since the UN SC Resolution 1325 (UNSCR 1325) on *Women, Peace and Security* was adopted. It establishes a strong normative framework for ensuring the needs, voices and perspectives of women and girls in preventing and settling conflicts, hence contributing to building up sustainable peace. The anniversary is a good impulse for reviewing the progress and the challenges in implementing the UNSCR 1325 and other related resolutions. Moreover, an international trend has been noted over the past years to acknowledge not only women's and girls' personal costs for the failure to protect them in the military conflicts' context, but also the extraordinary collective costs for the global community in achieving the objectives of peace building and post-conflict society reconstruction. The outcome of this acknowledgement was the adoption of a number of UN SC resolutions on *Women, Peace and Security*, national action plans, impressive speeches and structural changes setting the scene for real progress. And all this, because women's status in a country is a predictor of peace. Where women have few rights or opportunities to participate in decision-making, there are higher levels of violence and conflict. Changes in the treatment of women are among the first indications of instability (*Illustrated fact sheet of Women, Peace & Security by the Numbers*, 2008).

The Universal Declaration of Human Rights sets forth that *All human beings are born free and equal in dignity and rights* (art. 1). The societies with a high level of equality assurance indicator are associated with lower levels of different forms of conflict occurrence. The states with higher levels of equality between women and men prove to have a less violent behaviour within the state, and at the international level.

In the context of the current security environment, the states of the world have to cope with the crisis consequences provoked by the novel coronavirus (COVID-19) pandemic, which is an unprecedented global threat for social, economic and environmental security, as well as for national and international governance structures. Respectively, multiple pandemic implications are already felt in the implementation of *Women, Peace and Security Global Agenda (WPS Agenda)*. On the one hand, the mistaken perceptions regarding women's role in peace and conflict processes or the stereotyped perceptions regarding the gender perspective in security and defence sector are preserved. Besides, during the crisis periods, gender equality represents an objective which frequently is placed in temporary stand-by. The existing studies reveal that there might be the danger for escalation of such perceptions in conflict zones or even humanitarian crises might emerge, and in some countries the level of domestic violence has increased in the context of self-isolation measures. The international experience shows that women's involvement as leaders in decision-making process has contributed to decreasing the pandemic effects, like in Germany, Thailand, New Zeeland, Finland and other. Instead of engaging in a political campaign, the female leadership from these countries have promoted solidarity and compassion among their citizens.

Currently, although the issue of mainstreaming gender perspective in security and defence sector is on the national agenda, as well as on the agenda of regional and international security organisations, it is nevertheless a complex and highly discussed topic, because there are still difficulties in mainstreaming a concept which promotes equal opportunities in a working environment dominated, on the one hand, by masculinity, and on the other hand, by stereotypes related to frequently mistaken understanding of gender perspective. Hence, the activists, policy authors and law makers, concerned with ensuring a high degree of equality between women and men, have promoted mainstreaming gender perspective into the legislative agenda. Thus, this article will focus, first of all, on the legal-political framework determining the commitments of the states and other stakeholders in implementing the Global Agenda *Women, Peace and Security* and, secondly, will point out the factors determining mainstreaming gender perspective in the security and defence sector of the Republic of Moldova. The mainstreaming of *gender perspective* in a context of policies or programmes represents a strategy to cope with concerns and experiences of women, as well as those of men in all areas of activity (political, economic, societal, security etc.), benefitting equally from opportunities and responsibilities (*Law No. 5 on ensuring equal chances between women and men*, in Albu, Mârzac, Negru, 2018, p. 33)[1].

Gender equality policies are specially created to solve problems resulting from gender discrimination or inequality situations. Based on the topic of the article, we will focus on the policies referring to the security sector through the lens of WPS Agenda provisions' implementation.

[1] Note: for comparison, the exact translation on the official documents from Romania is *"mainstreaming approach for equality of chances and treatment for women and men"*. The official documents from the Republic of Moldova use *"complex approach of equality between men and women"*.

POLICY FRAMEWORK REGARDING THE GLOBAL AGENDA *WOMEN, PEACE AND SECURITY*

The UN SC Resolution 1325 on *Women, Peace and Security*, adopted on 31 October 2000, tackles directly the war impact on women and women's contribution to settling conflicts and achieving stable peace. Actually, the *"Beijing Declaration"* and the *"Beijing Platform for Action"* adopted in 1995 represent the starting point for a long-term women empowerment strategy and underscore women and armed conflicts as one of the 12 key action areas. They require greater participation of women in conflict prevention and conflict resolution, peacebuilding, governance and in the protection of women during armed conflicts.

It is for the first time in an international agreement, when the platform underlines the importance of tackling women's safety and contribution in relation to peace, security and development. The UNSCR 1325 (point 4) calls upon the Secretary General to extend the role and the contribution of women to UN field operations, especially among military observers, civil police, personnel for human rights and humanitarian personnel. In this context, it should be pointed out that one of the priorities of the National Army of the Republic of Moldova refers to Moldovan militaries' participation in peace-keeping missions, being thus an evidence of the state's aspiration to promote the ideas of peace, stability and security within the country, but also abroad, so as to become a state which contributes to enhancing peace, and 1.8% of all participants in such missions are women.

To facilitate the fulfilment of the objectives envisaged in the UNSCR 1325, each of the mandates of the resolution is linked with one of the four main pillars: *participation, protection, prevention and recovery (Annex 1)*. To implement the four pillars, the organisations and the states adopt, as a rule an *Action Plan* referring to UNSCR 1325 as well as other related resolutions. The prior recommendations made by UN regarding the development of national action plans underline the fact that they should observe other legislative frameworks and national policies for their subsequent enforcement. Because the states differ, respectively the gender issue is tackled differently (either conflict situations or cultural and religion peculiarities have to be taken into consideration), there is no homogenous set of policy tools for implementing the *WPS Agenda*.

As of 2008, the UN SC adopted a number of resolutions completing the provisions of UNSCR 1325 and developing mechanisms for implementing the general objectives of peace, security and gender equality *(Annex 2)*. These resolutions enhance the global commitments, existing treaties and conventions regarding women's rights during peace and conflicts, and set up the *Women, Peace and Security Agenda*, which recognises the urgent need to integrate gender perspective in peacekeeping operations, hence contributing to maintaining and promoting peace and international security.

In 2015, during the *UN General Assembly Session, a new Universal Agenda for Sustainable Development* was established based on the Millennium Development Goals and supplemented with new goals. The new Agenda envisaged for 2015-2030 suggests sustainable development goals (SDG) and strategic targets, which are integrated indivisibly in the three dimensions of sustainable development: economic, social and environmental. The new global trajectory of the Agenda is found as well in the *Strategy for Ensuring Equality between Men and Women in the Republic of Moldova (for 2017-2021)*, which stipulates equality assurance in rights and opportunities for women and men, including as well objective 4 on *ensuring gender equality in security and defence sector* (Resolution no. 259 on 28.04.2017).

Together with the UN SC resolutions, *the General Recommendation No. 30 on women in conflict prevention, conflict and post-conflict situations* (GR30), approved in 2013, provide to the states guidelines on legislative and policy measures, as well as other corresponding actions to fully ensure the duties to protect, observe and apply women's rights in preventing conflicts, in conflict and post-conflict situations. GR30 ensures the application of the *Convention on the Elimination of All Forms of Discrimination against Women (CEDAW)*, approved by the UN General Assembly in 1979, which is a comprehensive international treaty and aims to achieve gender equality, to ensure women's rights in all the areas of life and, in general, to improve conditions for women. RG30 and resolutions on WPS Agenda are mutually referring to each other and provide modalities for enhancing each other's implementation. The Republic of Moldova ratified CEDAW in 1994 (Resolution no. 87 on 28.04.1994).

On 21 March 2018, the Government of the Republic of Moldova has approved the *National Programme for Implementing the Resolution 1325 of the UN Security Council on Women, Peace and Security for 2018-2021* (hereinafter referred to as the Programme) and the Action Plan to enforce it (Resolution no. 259 on 28.03.2019). The mentioned programme is the tool setting forth the implementation actions, expected results and implementation indicators for UNSCR 1325 at the national level.

From demining to disarmament, demobilisation and reintegration (DDR), from elections to constitutional changes, from security sector reform (SSR) to justice transitory measures, from economic recovery programmes to initiative for long-term

prevention of conflicts, from negotiation of peace agreements to settling problems related to refugees and displaced persons, the UNSCR 1325 points out that women's participation is imperative. In this context, 84 states at the global level have developed National Action Plans to implement the UNSCR 1325 (National Action Plans for the Implementation of UNSCR 1325 on Women, Peace and Security, National-Level Implementation, 2020), recognising that it ensures gender equality promotion and women's empowerment within a peace and security framework relevant for all the security sector areas. The Government of the Republic of Moldova decided to develop and approve such a programme based on the fact that it committed itself to implement the UNSCR 1325 under the Individual Action Plan of Republic of Moldova – NATO Partnership for 2014-2016, on the one hand, and there were identified certain limits/barriers at the national level for ensuring an inclusive security sector, on the other hand.

Ensuring equal opportunities and treatment between women and men in peace and conflict situations seems to be an up-to-date topic at the international and regional levels and within such organisations, as NATO and EU. The policies for promoting gender perspective of these organisations contribute to deepening the gender equality efforts in the area of security and defence. Based on the international commitments to implement the WPS Agenda, the states try to increase women's role in civil and military structures at the national level. Acknowledging the importance of implementing the WPS Agenda, NATO issued the *Directive Bi-SC 40-1* on 8 August 2012, which suggests including the UNSCR 1325 and gender dimension in NATO command structures, including the measures on protection during military conflicts (BI-Strategic Command Directive (BI-SCD) 40-111).

The North Atlantic Alliance has adopted as well an Action Plan for implementing the WPS Agenda. The first plan was adopted in 2010, mainstreaming the UNSCR 1325 into the operations and missions led by NATO (*NATO Action Plan on Mainstreaming UNSCR 1325 into NATO-led operations and missions*). This plan includes clear actions to be undertaken by commanders of NATO-led operations in Afghanistan (ISAF) and Kosovo (KFOR). The last Action Plan was reviewed and approved in 2018, fully acknowledging the importance of women's active inclusion, participation, and role so as to cope successfully with the security challenges from the 21st century, and reconfirming NATO and its partners' commitment to observe the main principles of UNSCR 1325 (NATO/EAPC Policy on Women, Peace and Security, 2018). As well, NATO has updated its policy under the Euro-Atlantic Partnership Council (EAPC) from the UNSCR 1325 perspective (NATO/EAPC Policy for Implementing UNSCR 1325 on Women, Peace and Security, and related Resolutions, 2018). The general principles approved by NATO member countries and its partners for implementing the WPS Agenda: (1) *Integration* – ensuring that gender equality is an integral part of NATO policies, guided by effective gender mainstreaming; (2) *Inclusiveness* – promotion of increased representativeness of women within NATO and national armies; (3) *Integrity* – accountability on all efforts to increase awareness and implementation of the WPS agenda will be made a priority in accordance with international frameworks (Women, Peace and Security, 2019).

At the same time, we cannot neglect the fact that equality between women and men is one of the fundamental values of the European Union (EU). In 1957 the principle of equal pay for equal work became part of the Treaty of Rome, and in 2016 the *Strategic commitment for gender equality for 2016-2019* was approved setting forth the activity programme of the European Commission in relation to equality. Referring to the implementation of the UNSCR 1325 at the EU level, it should be pointed out that in September 2005 an optional document was approved regarding the implementation of the UNSCR 1325 in the context of the European Security and Defence Policy (ESDP). The document included recommendations on mainstreaming gender perspective at all the stages of ESDP missions/operations, from planning to reporting, and lessons learned. Based on this document, the European Council developed a *checklist*, which was adopted in July 2006. Besides, the Council adopted in November conclusions on mainstreaming gender equality in ESDP. Moreover, during the same year, the European Parliament issued a Resolution regarding women's situation in military conflicts and their role in the rebuilding of democratic process in post-conflict countries.

At the same time, the Gender Equality Promotion Commission has assumed itself the commitment to promote the *WPS Agenda* beyond the EU. This commitment is also found in the context of implementing the 17 Sustainable Development Goals (SDG) of the 2030 Agenda. Having a valuable experience in implementing the SDG 5 *Gender Equality* and SDG 16 *Peace, Justice and Strong Institutions*, EU supports the partner countries, such as the Republic of Moldova, in implementing the Agenda 2030 for *Fulfilling gender equality and capacitating all women and girls*, as well as *Promoting peaceful societies and favourable to inclusion for sustainable development, ensuring access to justice for all and creating efficient, accountable and favourable to inclusion environment, at all levels*.

NATIONAL FRAMEWORK FOR IMPLEMENTING THE UNSCR 1325: PERSPECTIVE OF THE REPUBLIC OF MOLDOVA

As mentioned previously, the four pillars for implementing the UNSCR 1325 facilitate the structuring of priority interventions or sector actions under the Action Plans for *WPS Agenda*. In reality, the UNSCR 1325 does not specify the reforms' content, the way in which they will be implemented or the necessary procedures for ensuring the implementation of provisions set within it. From outside, the UNSCR 1325 seems to be rather complicated than complex in relation to the internal dynamics of the states, hence leading to the question if the generic tools for mainstreaming the gender perspective may be applied efficiently in preventing and resolving conflicts as well as in post-conflict recovery (Barrow, 2009, p. 67). That is why the countries are encouraged to define exactly the relevant procedures in their action plans. The preliminary recommendations provided by the UN for drafting national action plans underline the fact that these plans should observe the national legislative and policy frameworks for their subsequent enforcement.

The national strategies or action plans for enforcing the UNSCR 1325 are relevant for all the countries, and not only for those involved in conflicts (*Preventing Conflict, Transforming Justice, Securing the Peace*, 2015). The states are frequently affected by conflicts with neighbours, countries from the same region or donor countries, involved in peacemaking efforts. Besides, the states are already reviewing how women, as human resources, should be included in the security structure at the national level. A number of studies have shown, for instance, that including more women in the military area and peacekeeping operations has increased considerably the efficiency of military operations' management (Olsso, Tejpar, 2012). This can be achieved by improving the acknowledgment and awareness level about the specific security threats. As a result, gender-sensitive policies are promoted to meet the different security needs. In spite of the adopted Programme and the initiated discussions regarding the COVID-19 pandemics' implications from the perspective of the different security needs, there are certain limits for acknowledging the need to implement the WPS Agenda.

In general, the legal-political framework for ensuring equality between women and men in the Republic of Moldova has been substantially improved over the past decades. Different legislative acts set forth provisions that directly or indirectly refer to non-discrimination and equality principles. These provisions are regulated both in the codified legislation (Criminal Code, Criminal Procedure Code, Civil Code, Civil Procedure Code, Contravention Code, Labour Code, Education Code and other), as well as in organic and ordinary laws of the Republic of Moldova. A brief analysis of the respective provisions and their compatibility with international standards may be found in the Legislative Report *Analysis of international standards and national legal framework in the area of gender equality in security and defence sector* carried out with the support of UN Women Moldova (Vieru, 2016, p. 96).

As for the *Strategy to ensure equality between women and men in the Republic of Moldova for 2017-2021* – it aims to empower women and fulfil de-facto equality between women and men in the Republic of Moldova. The main objectives of the strategy are to ensure complex approach to quality between women and men through women's participation in decision-making, to enhance the institutional framework for ensuring gender equality, to combat stereotypes in the society, to promote non-violent communication and to ensure gender equality in security and defence sector (Resolution no. 259 on 28.04.2017). In relation to security and defence sector, the Strategy stipulates a separate objective: General Objective 4. Promoting Gender Equality in the security and defence sector (Specific Objective 4.1: Ensuring women's access to management and execution positions in the area of security and defence; Specific Objective 4.2: Mainstreaming gender dimension in sector security and defence policies).

The *National Programme for implementing the Resolution 1325 of the UN SC on Women, Peace and Security for 2018-2021* is the tool establishing the implementation actions, expected results, and implementation indicators for UNSCR 1325 at the level of the Republic of Moldova Government, respectively at the national level. The aim of the Programme is to *express the organisational willingness of the institutions from the security and defence sector regarding the implementation and enforcement of provisions under the UNSCR 1325 and related resolutions and other complementary tools to ensure mainstreaming gender perspective within the respective institutions (see Chapter III – Institutional Framework) for carrying out the set missions*. To achieve the suggested goal, two basic objectives were set: (1) increasing women's representativeness in security sectors and (2) ensuring an inclusive security sector by implementing eight basic programmes adopted as eight objectives *(Annex 3)*.

The mentioned objectives were set as a result of the activity of the working group for Programme development. The need to develop a Programme at the national level was determined by the obvious existence of gaps from the sector's and society's perspective. After analysing the respective gaps/problems, eight basic barriers were structured: (1) Gender stereotypes about women's participation in the security sector still persist within the system (but also outside the system). (2) The security system does not allow men and women to reconcile the professional and family life. (3) The security system does not have full capacity to prevent and combat discrimination, harassment and gender-based violence. (4) The security system does not have an inclusive and pro-active human resources management system. (5) The security system does not apply reasonable adjustment and special temporary measures to allow a wider representation of women. (6) The security system is not transparent enough when it comes to the participation of the civil society, women's organisations and citizens. (7) The security policies are not gender responsive. (8) Limited policies for ensuring equal participation in peace-building and peace-keeping missions.

Every identified barrier is worth to be deeply analysed, because the institutions from the security sector have related, but nevertheless different missions, and the personnel status may be different or the activity programme is special. To this end, for instance, the problem of women's participation in peace-keeping missions is specific for the Ministry of Defence of the Republic of Moldova and maybe in future it will be a discussion topic for the Ministry of Internal Affairs. Women's absence in peace negotiations and in peace-building process is already a proved phenomenon, respectively there is a need to develop some policies for engaging women in the negotiation and mediation processes. Coherent and comprehensive approaches and strategies for enforcing the UNSCR 1325 become even more important when realities in the field are analysed. There is not yet a *"critical mass"* of women – negotiators and mediators to be involved in peace formal processes at the international level, as well as at the national level. The number of women-negotiators, mediators and signatories of peace agreements remains to be very small (*Facts and figures: Peace and security*, 2019). To a big extent, women's limited access to peace-building and negotiation processes as well as to decision-making process is also determined by the fact that there is no approach that would ensure the connection between presence and influence. Women's participation, without ensuring their influence, does not guarantee gender-sensitive peace agreements. Women have reduced access to formal institutions, power structures, monitoring mechanisms and funds, and remain to be widely excluded from implementing peace agreements.

Moreover, the gender-related problems are tackled as *"women's problems"* and not as structural issues of social justice faced by the society in general. These issues should be discussed in the context of specific legal, social and economic problems of negotiations – for instance, women's access to land rights should be discussed when negotiating the land rights and not only in relation to women's rights in general.

The fulfilment of the Programme's objectives contributes as well to increasing cooperation between ministries, with nongovernmental organisations and civil society, hence ensuring the visibility of actions carried out by the respective institutions in relation to implementation of the UNSCR 1325. Analysing the respective Programme from an academic perspective, it can be pointed out that it covers a synergy between the needs of the Republic of Moldova to implement the UNSCR 1325 and the four mentioned pillars. Although the UNSCR 1325 pillars are frequently used for organising priority interventions and actions in the national or sector action plans regarding the *WPS Agenda*, nevertheless there is no homogenous set of policy tools to implement the UNSCR 1325. As a rule, the stakeholders get adjusted to the four pillars depending on the identified problems and established priority areas.

Although the Programme is an essential tool or frequently the only bridge between the national and global levels for implementing the Resolution 1325, nevertheless such a Programme should not be the single modality of ensuring the continuity for implementing the *WPS Agenda*. The enforcement of the UNSCR 1325 at the national level could be carried out by changing, amending or adopting new internal legislative provisions. For instance, the *Law on Equality of Women's Rights* from Israel has included the mandate of having more women in peace negotiation, in line with the arrangements related to *WPS Agenda* (Hudson, 2013). It should be also mentioned that ambitious plans do not necessarily turn into efficient changes, if they are not drafted according to the national context, commitments, capacities and resources. As a rule, the results-focused actions are supported by political will, funds and commitment to changes tackling inequalities and structural exclusions in sustainable and effective ways (Swaine, 2015).

Actually, the development of an Action Plan to implement the UNSCR 1325 resides in its perspective to enhance and strengthen the obligations of the international law and, especially, the role of the *soft law* in promoting human rights among women and girls in peace and conflict situations. The notion of *soft law* is frequently used to describe different types of quasi-legal tools of the European Union: *codes of conducts, guidelines, communications* etc. At the same time, the national action plans for implementing the WPS Agenda are efficient tools for a better systematisation of the necessary activities to implement the four pillars of the UNSCR 1325.

INTERNAL AND EXTERNAL PERSPECTIVES ON IMPLEMENTING UNSCR 1325

Currently, it is considered that there is an obvious correlation between the gender equality indicators in the society and the level of ensuring the respective objective in the security sector, especially in a military institution. For instance, according to the study carried out by Mary Caprioli and Mark A. Boyer, it is less likely for the states having an increased level of gender equality at the national level to use violence in an interstate conflict (Caprioli, Boyer, 2001, pp 503-518).

As traditional gender roles still prevail in the Republic of Moldova, a woman's decision to teach in a military institution is intermediated in two stages. Firstly, the population perception on choosing an appropriate vocation for women, which would be in line with her socialisation and education in a specific gender role, and secondly, based on the institutional decisions of hindering their access.

Currently, there is more and more support for the fact that gender is a transversal analytical category, which should be applied to all the society development areas – political, economic, environmental, social, cultural and institutional. In this respect, the institutions from security sector are part of the governmental sector and interact with the society. But all institutions should take into account the fact that a *gender mainstreaming* strategy does not have a simple aim to produce documents that would include information about women and men and would provide evidence that a gender analysis was carried out, but also to lead to specific actions which would ensure an increased potential for promoting gender equality. This could lead to changes regarding the way in which: (1) objectives are expressed, (2) activities are developed and (3) anticipated results are defined (Hannan, 2000, p. 5).

The implementation of *gender mainstreaming* process needs a clear understanding about the gender perspective so as to determine its involvement in different areas and problems of the security sector. For instance, in relation to the issue of women in politics, it is important to understand the gender perspectives to be able to determine what actions should be undertaken to ensure equality between women and men at the decision-making level.

To include gender equality in general attention, *gender mainstreaming* should be tackled as a systematic strategy, meaning as a permanent objective of already existing public policies. For instance, the draft National Defence Strategy includes genders aspects in Chapter IV Resources for defence fulfilling, point 60 *"Mainstreaming gender perspective in the country's security and defence policies will be carried out in line with the needs to complete the national defence system with human resources, both during the peace time, but also during war/conflict* *times. At the same time, this fact will contribute to implementing the commitments assumed by the Republic of Moldova, regarding the Resolution 1325 of the UN Security Council"* (Hannah, Ibid.).

At the same time, it should be taken into consideration that mainstreaming gender perspective in the security sector does not mean just simple inclusion of more women in the sector. Although full and equal representation of women represents an important step towards ensuring gender equality, this does not ensure the fact that gender perspective is taken into consideration. Hence, gender mainstreaming has two dimensions specific for security sector: *internal and external*.

The internal dimension refers to the fact that gender mainstreaming represents a modality to encourage the institutions from the security sector (armed forces, public order and law enforcement structures) to base themselves on men's and women's capacities. Thus, in June 2018, the Republic of Moldova Government approved the *Professional Army Programme for 2018-2021*, which aims to prioritise the development areas of the defence sector (Resolution of the Republic of Moldova Government, 2018). As a rule, such processes may have a *structural effect*, one of the most visible being the *sharp growth of the need to increase the share of military women*. The reason is simple: all the people called upon to perform the compulsory military service in the Republic of Moldova were men. While the global figures show that the share of female personnel in uniforms may go up mechanically. That is why the defence sector should be ready to apply a gender-mainstreaming approach taking into account the staffing needs with human resources.

In this context, the need to increase women's proportion in the armed forces implies, first of all, gender by considering two aspects: (1) problems related to gender equality within an organisation, such as equal opportunities in relation to recruitment, advancement, work conditions etc. and (2) such topics as norms, attitudes, values, organisational culture and management styles. Both aspects have a direct as well as an indirect impact on the extent to which adequate attention is provided to gender equality problems in the basic activity of the organisation and in the ways in which such organisational factors as management styles, work styles and organisational culture may have an impact on the mainstreaming potential. Hence, whenever the organisational culture is low, it is more problematic for the military institution to achieve gender equality. That is why, frequently when mainstreaming gender perspective in internal strategies as a result of increasing women's number in the security sector, it is necessary to come up with training, for instance in preventing violence or sexual harassment at the work place.

Secondly, the *internal dimension* refers to mainstreaming gender both at the management and executive levels within institutions of the security sector. Thus, it should not be neglected that a gender-sensitive strategic management of human resources provides the basis for recruiting personnel with different qualifications, either females or males. For this to happen, the armed forces should conceptualise what gender perspective and UNSCR 1325 mean for them.

At the same time, in the context of national armed forces professionalisation, the transformation of the modality to plan and fulfil operations by the armed forces needs a strategic plan for all intentions that backstop gender mainstreaming – what are the goals and what do we do to achieve them, *who is responsible for achieving them*? Only in this case, the intentions of the strategies will be followed by actions that can facilitate the change e.g. allocation of financial resources for gender-related items, reporting of failures and successes, accountability of persons. For instance, some states establish such positions as ministers' gender advisors. In this respect, the neighbouring state would be an example, where the Ukrainian Ministry of Defence established a position which is responsible for ensuring equality in rights and opportunities for women and men in the Ukrainian armed forces.

Referring to the Republic of Moldova, besides those eight barriers mentioned in the Programme for implementing the UNSCR 1325, the limits for mainstreaming gender in security sector were also determined by the fact that *there is direct correlation with the barriers for women's participation in politics and in high-level decision-making process*. This fact limits the assurance of balanced participation, from gender perspective, in management positions within institutions of the security and defence sector, as well as the full involvement in the parliamentary committees responsible for security issues or within diplomatic missions (only seven women as heads of diplomatic missions in 2019).

The problem resides in the so-called vicious circle, meaning that gender inequalities on the labour market from the security sector also lead to unequal chances for women in decision-making process and vice versa, the lack of women in management and decision-making positions limit the adoption of relevant policies to ensure equal opportunities in recruiting women (*National Human Development Report 2016 – "Inequalities in Human Development"*, 2017, p. 100)[2].

[2] Note: In the Republic of Moldova, the *Law on Political Parties* does not contain provisions which would impose barriers for women's representation, but they are found in the mechanisms for setting the lists of candidates and in women's participation in political life, in general. A study from 2015 reveals that women-candidates were mainly concentrated in the second part of party lists, while the first part advantaged men; hence the first decile of places with real chances would include 11% men-candidates and only 5.9% women-candidates; the average positions held by a man-candidate is 5-10 positions closer to the head of the list. It is established positively that women's share for the first five positions has increased considerably (from 5.3% in 1998 up to 23.1% in 2014).

In this context, the data of the Gender Barometer are very relevant, as they confirm that the main causes for inequalities in women' and men's rights derive not only from women's social role of double tasks – to maintain the family and to raise the children (mentioned by 36.5% of respondents), but also the fact that *women are not promoted in management positions* (25%) (Gender Barometer. *How women and men participate in politics and decision-making processes?*, 2017, p. 25). Hence, as it was mentioned previously, according to the critical mass theory, as long as women represent a distinct minority in a specific community – in our case the security sector – it is less likely for the community norms to get adjusted to allow promoting them. For instance, when women have no access to specialised necessary facilities and services, they are less susceptible to get qualified for specialised tasks. Hence, women do not benefit from equal opportunities and respectively, *nolens volens*, they are isolated or have no access to administrative positions or are discouraged to get promoted in decision-making positions (*Moldova's Security Sector Institutional Self-Assessment from the Gender Perspective*, 2016).

The external dimension of the process of gender mainstreaming in security sector refers to increasing security level and efficiency of security structures. It means that security institutions, depending on their mandates, interact with civilian population. For instance, the police forces ensure public order or fight against domestic violence; the Customs ensure the economic security of the country by combating frauds at the state border, hence ensuring not only the security of the state, but also of the population. And the different security needs of women and girls, and men and boys, induce a gender-based approach of the institutional policies.

In relation to the military sector, these two dimensions, internal and external, are tackled in the specialised literature more frequently from the perspective of international operations. Externally, having a gender perspective improves the way we look at a society and therefore it enlarges our *"situational awareness"*. This creates a better understanding of culture, local customs and values. It can improve access to and communication with the local population, local government and the International Community. A proper gender analysis can be a force-multiplier and improve mission effectiveness. If conducted in the right way it should also include an internal focus, looking at our own internal procedures, policies, training means and assets (Groothedde, 2013, pp. 23-24) and other relevant practices in the process of localising security needs.

COVID-19 GLOBAL CRISIS AND IMPLEMENTATION OF *WOMEN, PEACE AND SECURITY* GLOBAL AGENDA

Currently, in the context of major challenges in the security area, more convincing findings emerge establishing that COVID-19 crisis has shown that women's leadership is an indicator of healthier and more equal societies, which are open to political agendas placing social and environmental wellbeing in the centre of national policies' drafting process (Conscieme et al.). In this framework, the statistical analysis of available data regarding COVID-19 pandemic, as well as the review of certain dimensions of basic human needs, inequalities and economic resilience, carried out under *Women in power: Female leadership and public health outcomes during the COVID-19 pandemic study* have pointed out important correlations, such as:

- The countries with women in leadership positions registered six times fewer COVID-19 confirmed deaths that the countries with male leadership;
- The governments led by women were more efficient and more rapid in flattening the epidemics curve, with daily death peaks six times smaller than in countries led by men;
- The average number of days with confirmed deaths was 34 in countries led by women and 48 in those led by men (Deane, 2020).

One of the study authors states that governments led by women shared similar approaches to the crisis, which are characterised by early consultation with experts and national advisors in health area, and isolation measures were implemented timely. On the other hand, the majority of governments led by men have reduced initial warnings and responded with substantial delays to the crisis. For instance, when on 14 March (with only 102 confirmed cases of novel coronavirus) the New Zeeland Government led by Jacinda Ardern announced strict lockdown measures, the British government led by Boris Johnson allowed during 10-13 March (with over 700 confirmed cases) mass gatherings of people in wide events, such as the soccer match of UEFA Champions' League, Cheltenham Festival, Crufts and other music concerts.

A similar positive model was noticed in Denmark, Norway and Finland – all of them led by women, unlike Sweden, where economic considerations have affected health concerns and, finally led to the highest number of deaths per capita in Europe. In spite of the general situation in the USA, one of the biggest leading state in the top reported coronavirus cases (*COVID-19 cases and deaths among hardest hit countries worldwide*, 2020), in California State, the mayor from San Francisco, London Breed, the first black woman who has ever had such a portfolio, has obtained advantages in managing coronavirus pandemic at the local level. The mayor undertook certain rapid prevention measures although there were still zero confirmed cases of coronavirus among San Francisco residents, and the global situation has changed rapidly (*City of San Francisco Moves Proactively to Prepare for Possible Novel Coronavirus Activity in the Community*, 2020).

In reality, these findings provoked multiple discussions and disputes at national and international levels, especially in the context of the approach that *female leaders see and manage the risks differently as compared to their male counterparts*. One of the disputes refers to the fact that some correlations do not necessarily represent the cause-effect relation and the leader is not a valuable determinant in combating COVID-19 pandemic or there are other more important factors, such as the culture of wearing masks in Taiwan. Indeed, when analysing the data about coronavirus spread and deaths caused by this virus, it is important to include in the analysis the following: population density, exposure to those who have travelled and the date when lockdown measures were applied. The first two indicators cannot be really influenced by leaders, while the date of the so-called *lockdown actions* is directly related to the actions undertaken by leaders. It is indeed presumed that the number of deaths caused by COVID-19 is substantially lower in the areas where leaders acted earlier, even one week earlier.

In this context, a number of researchers refer to the famous study from 1994 which has caused quite a stir by identifying what we call now *the white male effect* (Flynn, Slovic, Mertz, 1994). It seems that white men perceive health and technological risks as being low as compared to women and black persons. Developing this topic, it is considered that this is due to the fact that women, black persons, persons with disabilities are subject to daily risks, hence they have to cope continuously with some risks. That is why they perceive the risks differently and they act differently in relation to risks. Moreover, female leaders are more susceptible of being blamed if decisions are not popular or not efficient, or are always questioned for certain actions, and here we can provide Maia Sandu's example when her government was dismissed based on a non-confidence vote in November 2019. Due to these reasons, female leaders know that they need more *coverage* than men that have to be sure that their actions and policies are efficient. However, only 7% of the total number of state leaders are women.

Further to the above, there are already studies which point out that countries with women-led governments meet better the basic human needs, which is a component of the social progress index, encompassing aspects related to basic healthcare, sanitation, shelter and personal safety. Here, we do not talk about discrimination or diminishing the capacity of one gender as compared to the other, but it is rather outlining the correlation among general equality, *security culture* and *good governance*. The countries with female leadership are among the top countries with a high good governance indicator *(Good Governance study*, 2017) and high- performance score for *Women, Peace and Security index (Women, Peace and Security Index 2017/18)*, for instance Germany, Finland, Denmark, Estonia, Canada and other. In other words, the countries that have already a longer experience of mainstreaming gender in their security policies, namely gender stereotypes, are out of date and offer conditions for guaranteeing equal opportunities at all the levels, thus promoting inclusive governance, stability and prosperity.

Hence, COVID-19 pandemic does not cancel the implementation of security policies and strategies, including the *WPS Agenda*, but on the contrary, new solidarity efforts are needed to tackle the different security needs, respectively to have a more inclusive society. Moreover, COVID-19 has multiples implications on *WPS Agenda*. Directly or indirectly, the multidimensional nature of these consequences has an impact on international and national security, as well as on state security and individual security. For instance, the following has been noticed: (-) exacerbating disputes and rivalry among global stakeholders; (-) escalation danger for some local conflicts, as already existing studies reveal humanitarian crises in conflict zones; (-) long-term implications for national security and human security (financial crises, increase in political instability, review of security policies, reorientation of work practices). Counteracting risks and threats as a result of pandemic effects imposes the need to undertake some immediate or preventive measures, as well as to initiate actions for getting adapted to post-COVID-19 life by leveraging existing policies.

The pandemic contributes to aggravating the harmful perceptions regarding gender or leads to insufficient resources for implementing the Actions Plans under the WPS Agenda, as all the efforts are focused on the fight with COVID-19. Nevertheless, this pandemic is also an opportunity to challenge the harmful gender norms, as the crisis disturbs and brings light to many systemic and structural barriers which have impeded gender equality promotion. The already emerging examples include the binding teleworking measures adopted by numerous organisations from the entire world, thus opening traditional work places for the value and productivity of remotely working employees. Briefly, this lockdown could be a chance to switch to more flexible, more inclusive and more family-friendly jobs and a more balanced share of family and care responsibilities between working mothers and working fathers. For instance, in the context of COVID-19 crisis, the need has been acknowledged in the Republic of Moldova to apply more actively of the objectives set in the *National Programme for implementing the UNSCR 1325* *on Women, Peace and Security for 2018-2021*, especially the objectives 2 and 5, which refer to increasing the possibilities of women and men from the system to combine professional and family lives and to undertake special measures, such as flexible work programme or remote work.

Hence, based on the international experience, an inclusive governance that can get adjusted to new challenges contributes to increasing resilience, credibility and stability. The development of post-COVID-19 security culture will also depend on whether the different security needs were taken into consideration during the pandemic situation.

CONCLUSIONS

The value of the UNSCR 1325 for *WPS Agenda* is determined by the fact that this document has reaffirmed the importance of women's role in preventing and solving the conflicts and in the process of peace building; underlying as well the importance of increased women's role in decision-making in peace and conflict processes etc. Based on the international commitments to implement the *WPS Agenda*, the states try to increase women's role in civilian and military structures at the national level. The changing nature of modern conflicts and wars as well as their impact on civil population and especially on women determined the Security Council to recognise at the international level the fact that women's rights are excessively violated during conflicts; women become victims of different forms of violence, and the economic conditions get radically changed regardless of cultural and mentality differences.

The efficient implementation of the UNSCR 1325 and respectively of the *WPS Agenda* envisages, first of all, the development of an Action Plan. Many countries are testing their first plans, while others are implementing already the second or even the third generation of such plans. The Republic of Moldova's perspective to develop and implement a NAP for UNSCR 1325 is relatively new. Just like in the case of any public or national crosscutting policy, there are implementation challenges, but also achieved successes. Some plans do not have adequate resources (only 22% of adopted plans include an allocated budget for enforcing the NAP after its approval), are not politically supported, do not point out national priorities or are not personalised in the local context. They are *big on paper*, but do not have efficient mechanisms for coordination or accountability.

Hence, by drafting a political-legal framework for implementing the *WPS Agenda* through developing a National Programme, the Republic of Moldova would strengthen the implementation of the following commitments: (-) to intensify the strategic orientation of its efforts to implement the Resolution 1325 and (-) to develop and provide a new uniform reference frame for its actions/measures. In this process, the institution from the security sector, usually, hope to get additional synergy and mobilisation effects and to communicate more efficiently their activities among the interested public, as well as to international partners. On the other hand, a policy framework for ensuring a gender mainstreaming approach in the security and defence sector provides the national governments with: (-) an opportunity to go through all the policies of the *WPS Agenda* implemented by different governmental bodies, ensuring that Agenda's provisions are taken into consideration and no essential area is omitted, thus ensuring *supervision and comprehensiveness*; (-) an opportunity to have a *coordinated process so as to avoid doubling of efforts*, when expertise and knowledge are shared instead of being collected by every institution just for itself; (-) an information framework for relevant governmental stakeholders and civil society regarding the *WPS Agenda*, hence contributing to *increasing the awareness level*; (-) an opportunity de develop a wider accountability for *WPS Agenda – governance/ownership*; (-) tools to monitor the relevant actions *which* get to be identified and *who* should implement them, thus developing the *responsibility*.

A specific element for the Republic of Moldova is the fact that the approach through those eight barriers and two basic problems has facilitated the development of ministerial action plans depending on the institutional needs and capacities for ensuring gender mainstreaming, from the sector's internal perspective – increasing women's representativeness in the security sector, as well as the external one – ensuring an inclusive security sector. These two dimensions provided a major support for mainstreaming gender in sectary sector, either internally – meaning the institutional culture and work relations, or externally – security suppliers.

In conclusion, gender-sensitive policies and practices should be considered as a precondition for responding to challenges and will become a reflex for decision-makers involved in managing, preparing for, responding and mitigating crises. Moreover, the transforming vision of a post-COVID-19 world will be focused on people, prevention, peace, cooperation and human security. In this context, empathy, confidence and solidarity are necessary for a better understanding of the different security needs. The pandemic crisis has also pointed out the need to develop resilience and leadership spirit so as to become more adjustable, and leverage everybody's creativity and talent, by using new methods and practices for ensuring an inclusive security environment.

BIBLIOGRAPHY:

1. Albu, N., Mârzac, E., Negru, A. (2018). *Rezoluţia 1325 a Consiliului de Securitate al ONU privind Femeile, Pacea și Securitatea. Agenda Femeile, Pacea și Securitatea*. Guidelines developed within the project *Planul Naţional al Republicii Moldova de implementare a Rezoluţiei 1325 a Consiliului de Securitate al ONU*, supported by *NATO Programme Science for Peace and Security*. Chișinău.
2. Barrow, A. (2009). *[It's] like a rubber band'. Assessing UNSCR 1325 as a gender mainstreaming process. International Journal of Law in Context*. Cambridge University Press.
3. Caprioli, M., Boyer, M.A. (2001). *Gender, Violence, and International Crisis*. In: *Journal of Conflict Resolution*, vol. 45, issue 4.
4. Coscieme, L., Fioramonti, L., Mortensen, L.F., Pickett, K.E., Kubiszewski, I, Lovins, H., Mcglade, J., Ragnarsdóttir, K.V., Roberts, D., Costanza, R., De Vogli, R., Wilkinson, R. (2020). *Women in power: Female leadership and public health outcomes during the COVID-19 pandemic*. https://www.medrxiv.org/content/10.1101/2020.07.13.20152397v2.full.pdf, retrieved on 03 July 2020.
5. Deane, T. (2020). *Countries with female leaders suffer six times fewer COVID-19 deaths*. https://medicalxpress.com/news/2020-05-countries-female-leaders-covid-deaths.html?fbclid=IwAR38kupcryvag0Dad__o2Prl4BzRnR2wwNCfkY-DyqNu0kXWCZR4M0Ii8XU, retrieved on 04.07.2020.
6. Flynn, J., Slovic, P., Mertz, C.K. (December 1994). *Gender, Race, and Perception of Environmental Health Risks*. In: *Risk Analysis, an International Journal*, Volume 14, Issue 6. https://onlinelibrary.wiley.com/toc/15396924/1994/14/6, retrieved on 20 July 2020.
7. Groothedde, S. (2013). *Gender Makes Sense: A Way to Improve Your Mission*. Civil-Military Cooperation Centre of Excellence (CCOE).
8. Hannan, C. (2000). From concept to action: gender mainstreaming in operational activities. http://www.un.org/womenwatch/osagi/pdf/undppaper.PDF, retrieved on 24 June 2020.
9. Hudson, F.N. (5-7 November, 2013). *National and Regional Implementation of Security Council Resolution on Women, Peace and Security*. New York: UN Women Background Paper for Global Review Meeting, UN Women. http://www.peacewomen.org/assets/file/final_report_global_review_meeting_.pdf, retrieved on 24 June 2020.
10. Olsso, L., Tejpar J., eds. (2009). *Operational Effectiveness and UN Resolution 1325 – Practices and Lessons learned from Afghanistan*. Swedish Defence Research Agency Stockholm.
11. Swaine, A. *Implementing Resolution 1325: the role of National Action Plans*. (2015). https://www.opendemocracy.net/5050/aisling-swaine/implementing-resolution-1325-role-of-national-action-plans, retrieved on 24 June 2020.
12. Vieru, V. (2016). *Analiza standardelor internaționale și a cadrului legislativ național în domeniul egalității de gen în sectorul de securitate și apărare*. UN Women. Chișinău.
13. Whitman, T., O'Neill, J. (April 2012). *Attention to gender increases security in operations: Examples from the North Atlantic Treaty Organization (NATO)*. Washington: The Institute for Inclusive Security.

14. *Barometrul de gen. Cum participă femeile și bărbaţii în politică și în procesele decizionale?* (2017). Chișinău: Centrul "Parteneriat pentru dezvoltare".
15. *BI-Strategic Command Directive (BI-SCD) 40-111*. http://www.cimic-coe.org/wp-content/uploads/2014/06/20120808_NU_Bi-SCD_40-111.pdf, retrieved on 18 June 2020.
16. */Good Governance*. www.ssfindex.com/ssi2016/wp.../pdf/indicator9-2016.pdf, retrieved on 20 July 2020.
17. *City of San Francisco Moves Proactively to Prepare for Possible Novel Coronavirus Activity in the Community*. https://sfmayor.org/article/city-san-francisco-moves-proactively-prepare-possible-novel-coronavirus-activity-community, retrieved on 20 July 2020.
18. *Countries with female leaders suffer six times fewer COVID-19 deaths*. https://medicalxpress.com/news/2020-05-countries-female-leaders-covid-deaths.html?fbclid=IwAR38kupcryvag0Dad__o2Prl4BzRnR2wwNCfkY-DyqNu0kXWCZR4M0Ii8XU, retrieved on 04 July 2020.
19. *COVID-19 cases and deaths among hardest hit countries worldwide*. https://www.statista.com/statistics/1105264/coronavirus-covid-19-cases-most-affected-countries-worldwide/, retrieved on 20 July 2020
20. Regarding the approval of the Professional Armed Forces Programme. https://gov.md/ro/content/cu-privire-la-aprobarea-programului-armata-profesionista-2018-2021, retrieved on 24 June 2020.
21. *Universal Declaration of Human Rights*. https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/rum.pdf, retrieved on 12 June 2020.
22. *Facts and figures: Peace and security*. http://www.unwomen.org/en/what-we-do/peaceand-security/facts-and-figures, retrieved on 24 June 2020.
23. Government of the Republic of Moldova, Professional Armed Forces Programme 2018-2021. (2018). https://gov.md/ro/content/cu-privire-la-aprobarea-programului-armata-profesionista-2018-2021, retrieved on 24 June 20202.
24. *Republic of Moldova Parliament Decision No. 87-XIII of 28.04.1994 on Republic of Moldova's joining CEDAW*
25. *Strategy for ensuring equality between women and men in the Republic of Moldova for 2017-2021 and the Action Plan for its implementation*. Government Decision No. 259 on 28.04.2017. Official Gazette no. 171-180, art. no. 410, http://lex.justice.md/viewdoc.php?action=view&view=doc&id=370442&lang=1, retrieved on 14 June 2020.
26. *Illustrated fact sheet of Women, Peace & Security by the Numbers*. http://www.oursecurefuture.org/publications/women-peace-security-by-the-numbers, retrieved on 12 June 2020.
27. *Implementing Resolution 1325: the role of National Action Plans*. https://www.opendemocracy.net/5050/aisling-swaine/implementing-resolution-1325-role-of-national-action-plans, retrieved on 24 June 2020.
28. *Law no. 5 regarding gender equalityi. In: Albu, N. et.al. Rezoluţia 1325 a Consiliului de Securitate ONU privind Femeile, Pacea și Securitatea. Agenda Femeile, Pacea și Securitatea* (see note 1).

29. *Moldova's Security Sector Institutional Self-Assessment from the Gender Perspective*. (2016). Evaluation Report. Inclusive Security.
30. *National Action Plans for the Implementation of UNSCR 1325 on Women, Peace and Security*. http://www.peacewomen.org/member-states, retrieved on 14 June 2020.
31. *NATO/EAPC Action Plan for the implementation of the NATO/EAPC Policy on Women Peace and Security*. (2018). http://peacewomen.org/sites/default/files/NATO%20Action%20Plan.pdf, retrieved on 18 June 2020.
32. *Preventing Conflict, Transforming Justice, Securing the Peace. A Global Study on the Implementation of United Nations Security Council Resolution 1325*. (2015). UN Women. SUA. http://wps.unwomen.org/en, retrieved on 24 June 2020.
33. *National Human Development Report 2016 Inequalities in Human Development*, UNDP Moldova, Chisinau, 2017.
34. *Women in power: Female leadership and public health outcomes during the COVID-19 pandemic*. https://www.medrxiv.org/content/10.1101/2020.07.13.20152397v2.full.pdf, retrieved on 03 July 2020.
35. *Women, Peace and Security*. https://www.nato.int/cps/en/natohq/topics_91091.htm?selectedLocale=en, retrieved on 18 June 2020.
36. *Women, Peace and Security Index 2017/18: Tracking Sustainable Peace through Inclusion, Justice, and Security for Women*. (2017). Washington, DC: Georgetown Institute for Women, Peace and Security and Peace Research Institute Oslo. https://giwps.georgetown.edu/wp-content/uploads/2019/11/WPS-Index-Report-2017-18.pdf, retrieved on 18 June 2020.
37. https://gov.md/ro/content/cu-privire-la-aprobarea-programului-armata-profesionista-2018-2021, retrieved on 24 June 2020.
38. http://lex.justice.md/viewdoc.php?action=view&view=doc&id=370442&lang=1, retrieved on 14 June 2020.
39. http://lex.justice.md/md/374810/, retrieved on 14 June 2020.
40. https://www.nato.int/cps/en/natohq/topics_91091.htm?selectedLocale=en, Women, Peace and Security. (2019), retrieved on 18 Junee 2020.
41. http://www.peacewomen.org/assets/file/final_report_global_review_meeting_.pdf, retrieved on 24 June 2020.
42. http://www.peacewomen.org/member-states, retrieved on 24 June 2020.
43. http://peacewomen.org/sites/default/files/NATO%20POLICY.pdf, retrieved on 18 June 2020.
44. http://peacewomen.org/sites/default/files/NATO%20Action%20Plan.pdf, retrieved on 18 June 2020

ANNEXES:

Annex 1. Pillars of Resolution 1325 on *Women, Peace and Security*

PARTICIPATION	Requests increased participation of women (•) at the decision-making levels, including in national, regional and international institutions; (•) within mechanisms for preventing, managing and settling conflicts; (•) in peace negotiation; (•) in peace building operations, as soldiers, policemen and civilians; and (•) as special representatives of the UN General Secretary.
PROTECTION	Requests especially women's and girls' protection against sexual and gender violence, including in emergency and humanitarian situations, such as refugees' camps.
PREVENTION	Requests for improvement of intervention strategies (•) to prevent violence against women, including through criminal investigation of persons responsible for violating international law; (•) to enhance women's rights based on national legislation; (•) to support local peace-maintaining initiatives and conflict settlement processes.
RECOVERY	Requests promotion of rescue and recovery measures to tackle the international crises through gender lens/dimension, including by observing the civil and humanitarian nature of refugee camps, taking into consideration women's and girls' rights while designing the respective refugee camps and settlements.

Annex 2. UNSCR on Women, Peace and Security

Resolution 1325 (2000)
was the first to tackle the different and sometimes unique impact of military conflicts on women
Resolution 1820 (2008)
recognises sexual violence as war tactics and mentions that rape and other forms of sexual violence may be war crimes, crimes against humanity or an element of genocide.
Resolution 1888 (2009)
focuses, as well, on the problem of sexual violence in military conflicts; provides for new mechanisms under the UN system; reiterates that one of the important objectives is to promote women's participation in negotiations and to increase their number in UN missions.
Resolution 1889 (2009)
calls upon the member states to promote women's participation in processes of political-economic reconstruction and decision-making.
Resolution 1960 (2010)
points out the importance of gender-disaggregated data of reference regarding the impact of conflicts; sets forth institution tools for combating impunity, presents the specific stages necessary for prevention and protection against sexual violence in conflict situations and sets forth the sexual violence consequences.

Resolution 2106 (2013)
points out the importance of guaranteeing criminal investigation of sexual violence acts, with the aim to combat the widely spread impunity for this crime.
Resolution 2122 (2013)
introduces measures for ensuring the participation and leading role of women in preventing conflicts, peace processes and all the measures for post-conflict recovery.
Resolution 2242 (2015)
encourages the member states to ensure the strengthening of Resolution 1325 and underlines repeatedly the importance of women's involvement in preventing and solving conflict and building peace.
Resolution 2272 (2016)
calls upon the member states to ensure the eradication of sexual exploitation and violation committed by persons involved in peace keeping missions and punishing the abusers.
Resolution 2282 (2016)
expresses concerns regarding the costs and increase of human suffering caused by military conflicts, underlines that a comprehensive approach to transitory justice and responsible security sector are essential for enhancing peace, reducing poverty and impeding the states to relapse in conflicts.
Resolution 2331 (2016)
the first resolution regarding trafficking in human beings which has condemned the phenomenon and pointed out how trafficking in persons may aggravate the conflicts and favour insecurity.
Resolution 2467 (2019)
refers to sexual violence in conflict and was voted with 13 „pro" votes and two abstentions (China and Russia).
Resolution 2493 (2019)
requested additional information regarding the progresses and disadvantages from the WPS agenda, as well as recommendation for tackling new and emerging challenges.

ANNEX 3. Programmes/Objectives in implementing the National Programme regarding the UNSCR 1325

PROGRAMME 1. ***Reducing stereotypes related to women's role in security sector*** aims to increase women's participation in peace and security processes by promoting security culture at the institutional, local and national levels. Women's visibility from the sector at the national level, awareness raising campaigns regarding the Resolution 1325 at the local level and periodical trainings regarding gender equality will contribute to increase the positive perception of women's involvement in the security sector, and this the level of population confidence will increase for security institutions.

PROGRAMME 2. ***Increasing the possibilities for women and men from the system to combine professional and family lives*** will allow reviewing at the institutional level the opportunities for introducing options of flexible working hours for women and men – parents from the system, as well as other measures that would allow men and women from the system to get more involved in the family life. The actions from this programme also aim to diminish the factors that contribute to women's mistrust in their forces in a system dominated by men or not friendly and not open to women.

PROGRAMME 3. ***Preventing and combating discrimination, harassment and gender violence in the sector*** envisaged to ensure the development of institutional capacities in this area, by developing policies, establishing **internal procedures** for reporting cases of harassment and violence etc., preventing and combating discrimination. The respective programme will contribute to decreasing the risks of emergence of situations of discrimination and sexual harassment in the context of increasing the number of women in the security sector.

PROGRAMME 4. ***Developing an inclusive and pro-active system for human resources' management*** will ensure the operation of institutions from the security sector, taking into account the non-discrimination and gender equality principles, hence contributing to increasing personnel and women maintenance in the security system. One of the aims of the programme is to enhance transparency and integrity of the system for career promotion.

PROGRAMME 5. ***Implementing reasonable adjustments and special temporary measures in the security system*** will allow applying some specific actions for wider representation of women in the sector by reviewing certain recruitment requirements, adjusting the needs from system infrastructure, and initiating internal programmes for mentoring and leadership dedicated to women from the system.

PROGRAMME 6. ***Enhancing transparency and involving civil society in decisions adopted by the security system*** will facilitate communication between the security institutions and civil society regarding gender topics in the sector of security and defence. As well, the respective programme represents visible premises for creating a consultancy platform for the institutions from the security sector with the civil society, as well as for creating partnerships with organisations from the area of women's rights and human rights.

PROGRAMME 7. ***Developing the institutional capacities for mainstreaming gender and security policies*** aims to raise awareness about the policies in the security sector regarding gender equality, taking into account the different needs of women and men in the security area. The programme will ensure the establishment of an internal procedure for ensuring mainstreaming gender equality in security policies and reviewing the needs for appointing gender units within security sector institutions.

PROGRAMME 8. ***Increasing women's participation in peace enhancing and peace keeping missions*** responds to the obvious need to encourage through different mechanisms women's participation in peace and security processed at the regional and international levels. This programme aims to set up a programme for reintegration and rehabilitation of militaries (men and women) who have participated in peace-keeping missions.

THE ARCTIC SECURITY SYSTEM – THE STAKES IN THE BATTLE FOR POWER –

Cătălin-Gabriel DONE, PhD Student

University of Naples “Federico II”, Italy

The transformations within the international system and the European security environment have necessitated the approach of alternative perspectives concerning the Far North. Today, the Sector Theory, which sets the limit of the sovereignty of riparian states over the Arctic region, no longer seems to properly provide a balance of power and security in northern Europe.

The article uses techniques of qualitative methodology to explore the consequences of the new geopolitical evolutions in the Arctic Ocean and their impact on the European security system, but also the specific way in which the Arctic Ocean has become, in recent years, a specific region of the confluence of strategic interests for the Russian Federation, on the one hand, and the Scandinavian states, the EU and NATO, on the other hand.

Keywords: Arctic Ocean; NATO; geopolitics; Russia; Scandinavia;

INTRODUCTION. ARCTIC SECURITY

As a periphery of the European continent, the Arctic security system has been constantly under pressure from the geopolitical game, especially once the profound effects of global warming began to be visible on the ice cap.

The climate change and the melting of glacial conglomerates have taken back on the chessboard of international relations the importance of territorial division and the influence exerted on vital geostrategic points, especially as the opening of a new maritime route linking the Pacific Ocean to the Atlantic by reducing the sailing time would bring many advantages, both economic and strategic.

Thus, the Murmansk-Vladivostok and Atlantic-Pacific shipping lines will become even more important, especially since the two principal routes will serve the future secondary trade lines, their control being vital for the world economy and European security.

The Arctic region acquires identity valences in the context of perpetual transformations in the foreign policy of riparian states, which tend to change the legal norms of international relations. The actions and the instruments used by them infringe, on the one hand, both the legitimate interests of other states and the self-censorship and mutual censorship imposed by international law, and, on the other hand, the jus cogens rules by applying other rules[1].

The transformations within the international system and the European security environment have forced the approach of some new perspectives concerning the Far North, the Arctic becoming the centre of gravity of new continental military doctrines, the aggressiveness of the Russian Federation being the main element of new geostrategic arrangements.

As *“the rules governing the principle of recognition regulate, in most cases, the issues that arise in connection with the acquisition of international legal personality”* (Anghel, 2002), the Arctic territory is subservient to possible absorption by involving the interests of state actors in the region. This hypothesis is not recent. With the formulation of the thesis *Inledning till Sveriges geografi* by Rudolf Kjellen, the geographical space becomes vital for building a coherent foreign policy and a defence plan capable of ensuring strength and promptness in the event of an attack.

The multi-perspective on the Arctic security system traditionally derives from the cooperation force of the riparian states and from their attempt to draw their protection model, given their doctrinal antagonism.

[1] Which no longer has the same character, as stipulated in Article 53 of the Vienna Convention.

As power has consolidated the international relations, the nation-states have been in a constant arms race, with their military manoeuvrability based on unrestricted access to resources. Initially, the power represented the fullness of the state capacity and sovereignty (Kaviani, 2017) only later the scholar interpretations considered it *"an actor's ability to cause others to do something they would not otherwise do*" (Keohane & Nye, 2009).

In this manner, since the 18th century, a chain of systemic approaches to security has established in the Arctic region. These have allowed the residents constantly to exercise control over the waterways, but also to ensure their protection needs.

The Great Northern War properly provided Europe with a new security system that remained undisturbed until the beginning of World War I – the Arctic represented the delimitation of spheres of influence in the North, a central balance of power that ensured a unanimously recognised geopolitical order.

Seen as a contemporary pivot of the global geostrategy, the Arctic becomes a multipolar nexus, the reasons that guide the ideologization of the Arctic security system being intimately linked to the prospect of access to some of the most massive deposits of hydrocarbons, drinking water, and minerals (Șișcanu, 2015).

So, the logic of the conflict becomes extremely realistic, the struggle for survival in the international system as well as the assurance of the necessary security turning the Arctic continent into a global element, which offers optimal possibilities for both cooperation and confrontation. It should be emphasised that the geopolitical components of the Arctic are completely spontaneous and unpredictable, which makes it relevant both regionally and internationally.

As Russia has constantly been seeking a strategic depth to deal with any threats, the Arctic has represented a buffer zone that has allowed it to stabilise its northern border and ensure no one will invade it from this part of the globe (Marshall, 2019b). At the same time, beyond their traditional territory, the Scandinavians are trying to consolidate their position of power in the Arctic Ocean, offering new regional power structures capable of limiting any attempt to assert the Arctic hegemony. Nevertheless, there is something deeper in the interest of riparian states in what is invariably happening in the Arctic. China is becoming increasingly so aggressive on the international stage, and the adoption of its own Arctic policy proves its ambitions as a relevant player in the polar region (Koh Collin, 2020). Let us not forget that the executive Beijing authorities managed to obtain the observer status in the Arctic Council after a Norwegian island hosting a Chinese research base (Marshall, 2019a).

At this time, the forms of regional cooperation have managed to ensure a balance of power in the Arctic, with the elaborate security system remaining unaltered, although *"the local rivalries persist"* (Østhagen, 2019). The military manoeuvrability is invariably becoming an extremely insolent measure, giving rise to regional tensions with profound effects on global security.

THE SYSTEMIC RISK FACTORS AND THE DYNAMICS OF THE ARCTIC NEXUS

The challenges to the European security caused by the violation of Ukraine's territorial sovereignty by the Russian Federation, as well as its armed aggression, show us Russia wants to be recognised, not just declaratively, as a great power. As a result, we were in a situation where *"a nuclear state raised against a state the size of France, a dictatorial government against a revolutionary one"* (Krastev, 2014). But the whole event of occupying part of the territory of a sovereign state, the successive violations of international law, ignoring any norms of conduct in the system, represent just a few key elements of the structural-social identity of the Russian Federation (Morozov, 2015).

The competitiveness of the contemporary multipolar system has determined the Russian Federation to be extremely attentive to its pecuniary interests, the counterbalance of the balance of power being its primary goal. Therefore, the *"strategic identity"* of the Russian Federation became an extremely critical component, its long-term thinking changing radically – from *"a self-sufficient international actor"* to one *"who had to rethink his political organization in-depth, and economic"* (Garnett, 2008). This strategic perspective forces the Russian state to obtain its buffer space to ensure its control over the spheres of influence, as well as the connection channel with more *temperate waters*.

The geopolitical and geostrategic realities of the moment reveal new components of the state security system. According to Barry Buzan (Buzan et al., 2011), a security complex involves the politics, the combat capability, the economy, the society, and the environment, all of which remain extremely critical elements for the survival of the state and the design of its strength within the international system. If we will analyse this set of elements, we will notice that Russia's strategic pivot is the Arctic continent, which ensures its multilateral approach to its power.

The militarisation of the Russian region bordering the Arctic Ocean causes sudden changes in the balance of power in the area – *"an armed unit with at least 6,000 troops is being trained in the Murmansk region and which will include two mechanised infantry brigades"* will ensure the need for Russian stability in the far North (Marshall, 2019a).

The Arctic Nexus has become an arena of geopolitical games, the recent evolutions of the Arctic Ocean explorations revealing that approximately 30% of world gas deposits and 13% of oil ones are in this area (Ghimiș, 2011). As a regional energy hub with international values, Murmansk province can provide to the Russian Federation an upward economic course, especially if the hydrocarbon and mineral exploitation become viable in the next ten years. In this manner, in the Arctic region, we witness the formation of the influence triangles, the periphery of the international system becoming the arena of a zero-sum game, in which there is only one winner, the others being the losers of the power race (Ghimiș, 2013).

However, not just the resources are a huge stake for the riparian state actors, but also the development of a maritime alternative in the North Arctic Ocean that will not only reduce transportation costs but as well increase the transportation system security. However, *“the navigation in these waters requires high technology, infrastructure, and coordination to counteract the effects of the Arctic environment on intercontinental voyages”* (Cățoi, 2014), which the Russian Federation understood, the development of a comprehensive hydrocarbon processing system and transporting them from the far north to the European continent indicating the beginning of a new race for supremacy. On the other hand, the Russian territorial claims are becoming extremely problematic for the riparian states, as Russia’s exclusive control over the Arctic sea route could unbalance the entire Nordic security system.

As the geography realities impose on us the expanding of the North American and Eurasian continents into the depths of the Arctic Ocean (Laverov et al., 2013), the substantial changes in the Arctic strategic environment force the riparian states to consolidate their power so that these systemic risk factors do not threaten them.

In terms of Scandinavian security, Norway, Denmark, Iceland, Sweden, and Finland seem to understand that, from a strategic point of view, they play a key role in the European geopolitical stability. Being at the forefront of the fight for the Arctic, the Scandinavian states have precisely defined the entire region as a key priority of foreign and security policies, NATO having the role of ensuring, for the most part, the balance of power.

Another systemic risk factor for the Arctic is China’s expansionist policy. Considered to represent its distinct neighbourhood (The State Council of the People’s Republic of China, 2018), the Arctic has entered the sphere of Chinese influence due to Beijing’s desire to contribute to the development of research in Arctic ecosystems, meteorology, and marine resource management (Ibid). But the emergence of the Arctic at the international level can give China the strategic advantages needed to face its main rivals. For a notable example, the energy cooperation between China and Russia in the Arctic will naturally lead to a major decrease in China’s massive dependence on the energy production, with Chinese companies being extremely active and competitive in the Russian energy market (Koh Collin, 2020).

The potential of the Chinese presence in the Arctic is considerable. The energy projects as well as the development of telecommunications channels in the Arctic Ocean are causing enormous controversy among NATO, especially since the rivalry between the US and China has reached its peak. The Chinese military and economic

capabilities provide a dominant position to it, concerning the Arctic intraregional relations, *“the development of the Chinese infrastructure in the Arctic leading to a constant presence of China in the region”* (Yun, 2020).

Moreover, the Sino-Russian cooperation carries out an extensive role in destabilising the Arctic security complex due to its antagonistic position towards NATO in general and the USA in particular. Such mutual cooperation would jeopardise not only the authority relations but also the principles of international law that govern the Arctic affairs, and the Chinese presence in the Arctic Ocean could degenerate into an attempt to polarise the power source, just as in the South China Sea.

It is easy to understand if we will look at the fact that the current conditions of the Arctic environment allow the passage of the polar route in time with 40% shorter than the traditional one, through the Panama Canal (Marshall, 2019a). Thus, from an economic point of view, the Polar Route would allow China to require a significant leap and strengthen its dominance over Europe, and Russia would ensure, under conditions of force, rapid access to the temperate waters.

All these elements extensively represent a continuation of the arms race because the Russian-Chinese alignment against the West is making the Arctic nexus the scene of an ideological confrontation. Based precisely on three strategic levels of analysis – the raising awareness of the importance of the Polar region, the increasing of regional resilience, and also the strengthening of the international principles of Arctic governance, the US Department of Defense expressed their hard-line stance on the evolution of the Arctic environment (The US Department of Defense, 2019). Therefore, the critical events taking place in the Arctic Ocean directly influenced the national security system as well as the defence strategy of NATO.

From a military point of view, NATO seems to be leading the race for the Arctic, despite the declining US military presence in the area. In part, to maintain a balance of power, but also to defend its legitimate economic and security interests, the United States of America is encouraging the Scandinavian states to continue to increase their military capabilities in the Far North.

The Russian Federation recognises that the geographical element does not help it strategically because it has prevented the Russian naval military force in the Baltic Sea from maximising its power – because of both NATO’s exclusive control over the Skagerrak and the lack of a deep strategic corridor. Therefore, an armed attack can prevent Russia from a strategic reorganisation.

In this case, consider the possibility that the Russian authorities would become extremely offensive to be very high. The Northern Fleet, part of the Murmansk Region Joint Strategic Command, which owns about two-thirds of Russia’s nuclear

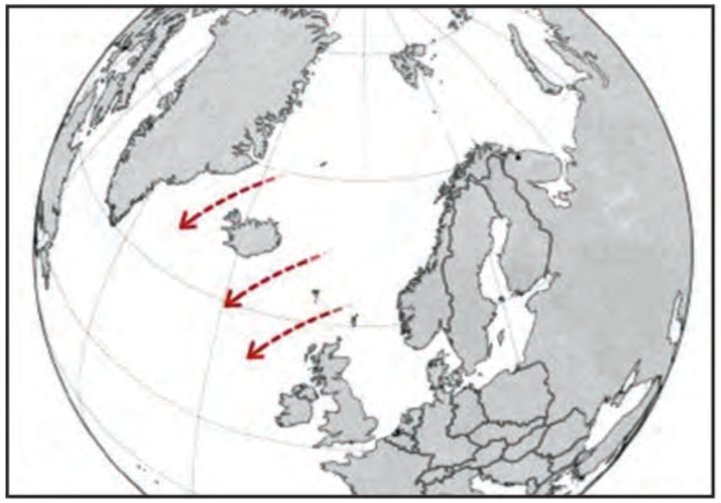


Figure no. 1: GOUK Strategic[2]

military arsenal (Интерфакс, 2016), would not have ample room for manoeuvre – *"only 290 km of water without sludge, from the Kola coast to the Arctic ice sheets"* (Marshall, 2019a). Thus, to reach the Pacific Ocean, the Russian fleet would have to enter in the Norwegian Sea and then to cross the GIUK strategic corridor, which would place it inferior to potential enemies.

Even if Russia is the largest polar power, it becomes increasingly clear that, without multilateral cooperation, the Scandinavian Euro-Atlantic integration can annihilate the strategic interests of Russians in the region. Also, the USA and Canada as a nearby neighbourhood ensure a brake in the Russian ambitions.

However, the issues of sovereignty and territorial claims are an obstacle to loyal cooperation. According to Kristian Åtland, the Arctic region comprises several variables that can redefine the northern security environment; judging by the energy, economic and strategic potential of the Arctic Ocean, confrontation is a reality (Åtland, 2013).

A various number of disputes can lead to a multi-level war. The elements as the delimitation of the continental shelf and the exclusive economic zones in the Barents Sea between the Russian Federation and Norway, the international status of the Svalbard archipelago, or the delimitation of the Arctic continental shelf beyond 200 nautical miles, as well as the delimitation of the Bering Sea are traditionally outbreaks of tensions.

[2] No More Pencils, 2018.

The global warming threatened the Arctic – as *"the average annual temperature has increased almost twice as much as in the rest of the world"* (Corell, 2006), the geographical factor has changed, causing problems related to territoriality to the bordering states.

The rising sea levels will bring serious problems to the region, especially as efforts to change social behaviour are needed. Thus, the imposition of coherent public policies that would allow the sustainable development of the region is necessary. Besides, the reduction of the annual amount of greenhouse gases affected the whole globe, especially the Arctic states.

The overall impact of the effects of global warming is huge. The extreme weather events destabilised the last frontier of the European continent, while the possibility of disappearance of the island areas became a reality. At the same time, the underdeveloped or developing area will suffer the most from the negative impact of global warming on the environment, and the global competitors fierce the fight for access to resources.

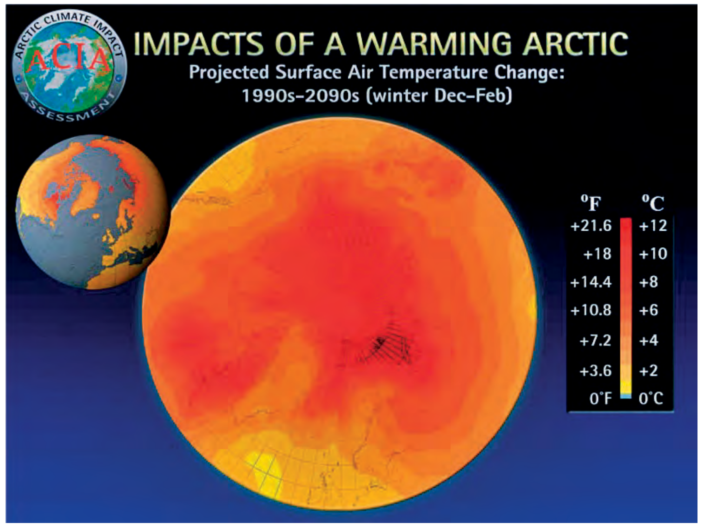

ARCTIC CLIMATE IMPACT ASSESSMENT
ACIA
IMPACTS OF A WARMING ARCTIC
Projected Surface Air Temperature Change:
1990s-2090s (winter Dec-Feb)
°F °C
+21.6 +12
+18 +10
+14.4 +8
+10.8 +6
+7.2 +4
+3.6 +2
0°F 0°C

Figure no. 2: The impact of global warming over the Arctic Region[3]

The radical transformation of the region exposed the Arctic security complex. Firstly, the possible opening of new navigable canals put the riparian states in front of systemic challenges, terrorism, organised mafia, and smuggling being systemic risks that the bordering states have not faced from the north.

[3] Corell, 2006.

Secondly, the issue of the continental shelves and the exclusive economic zones set by the melting of glaciers can be a potential *casus belli*. Thus, a combination of destabilising, multipotent factors that risk turning the Arctic security complex into a global problem. The internationalisation of the Arctic region would unbalance the power relationship between the two blocs that seem to face each other in search for assertion of the Arctic supremacy.

THE NUCLEAR ARGUMENT – A MODEL OF INTRA-REGIONAL COOPERATION

The decrease in the economic power has a direct counterpart in the decline of military response capacity. The prospects of the economic crises facilitated the illogical actions of states in their attempt to ensure their survival.

Daniel Dăianu, a member of the Romanian Academy, remarks in one of his analyses the fact that a geopolitical confrontation in the North would affect the Scandinavian and Baltic states (Dăianu, 2015). Time is an essential variable in the Arctic geopolitical game. The lasting confrontation also requires a large volume of liquidity allocated to defence and armament policies, which at some point can lead to the collapse of an entire system.

Since the beginning of the Cold War the nuclear argument has played a key role in the structure of global power. This is because the owners of nuclear warheads and the potential owners have continued the race to accumulate power to ensure the vital need for security.

The exercise of sovereignty in one's name over the Arctic region was not possible (Niemeschi, 2018). But under given conditions, this approach can no longer be excluded, the physical and natural factors obliging competitors in the international system to adopt new forms of behaviour.

"In practice, discouragement can be an institution and a set of strategies" (Zodian, 2013). This is why nuclear logic and the threat of total destruction ensure mutual respect for the orders in the system. Thus, the conflictual relationship between the riparian states has characterised the Arctic security environment but, at the same time, the certainty persists that the nuclear weapons will not be used by the combatant part. Even if the Russian nuclear arsenal persists as a powerful sign of offensive behaviour, the national authorities understand that resorting to a nuclear-armed attack would have irreversible consequences.

Based on the estimates made by Hans Kristensen and Matt Korda, we observe a relative uniformity of the distribution of nuclear power among the Arctic states (Kristensen&Korda, 2020).

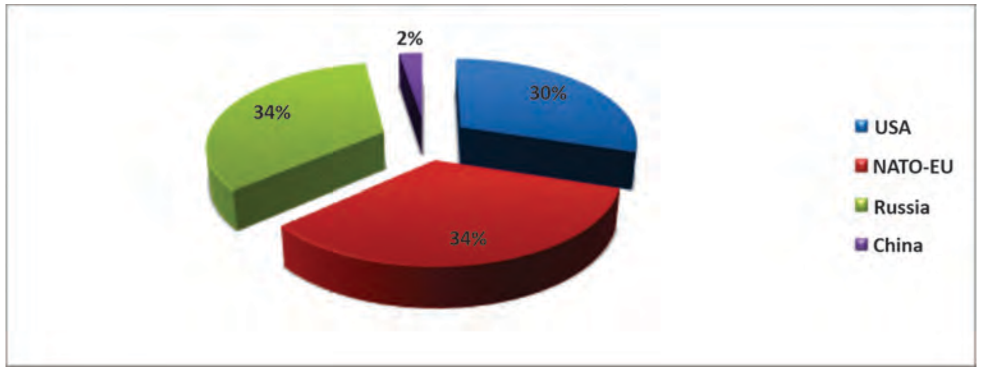


Figure no. 3: The distribution of the operational nuclear warheads between the Arctic powers[4]

Thus, benefiting from an equal response force, both Russia and the USA (and implicitly NATO), will call for intra-regional cooperation to resolve any disputes, and also to support the joint development and research projects. The projects such as Karelia CBC or Kolarctic CBC become vital for the security of the Arctic nexus and thus for the entire coastal region. Moreover, the cooperation within the Arctic Council ensures, with soft-power methods, an extremely important component of the regional power balance.

CONCLUSIONS

The adventurous spirit of the great powers to accumulate as much force as possible still governs the arena of international relations, the conditional ties of the moment imposing a complete reorganisation of the act of international governance.

The Arctic geography becomes, from one moment to another, an element of maximum importance in the development, adoption, and implementation of the defence and security strategies of the bordering states as well as of the expanding powers. The Arctic Ocean thus becomes the focal point of contemporary world politics. Even if the USA seems to be missing from the power equation, the battle for control of the new rimland is extremely tough.

The Arctic continent, as a geographical extension of the Eurasian coastal zone, becomes the core of the multi-level relations, its control ensuring naval supremacy (both military and commercial), as well as the prospects of thriving trade.

Moreover, the Arctic shipping routes will become part of an unpredictable game of power, the collective effort to ensure a balance of forces requiring compliance with international norms, as well as a rapid overhaul of geostrategic interests.

[4] Kristensen & Korda, 2020.

The foreign policy options and the military doctrines of the bordering states will decisively influence the ideological relationship between the two blocs – NATO and a possible Russian-Chinese alliance. Regarding these aspects, the Arctic vast territory can become a part of the sphere of hegemonic influence of an actor with considerable powers, but the importance of maintaining a relatively high degree of independence is essential to prevent a military confrontation.

The energy resources are the main stake of the confrontation for the region, as multiple forms of regional cooperation can ensure a continuity of geostrategic dynamics. Any logical fracture in the Arctic geopolitics unbalances the balance of power, forcing the adversary to react promptly and forcefully.

Thus, the Arctic security system becomes a vital component for the Euro-Atlantic complex, the defensive policy of the bordering state actors as well as the Chinese offensive having a major impact on the Arctic tactical field. The security dilemma of the Arctic nexus varies over time, being a result of intraregional relations.

BIBLIOGRAPHY:

1. Anghel, I. (2002). *Aspecte privind statul ca subiect de drept internațional*. In *Subiectele de Drept Internațional* (IInd, pp. 255-307). Lumina Lex.
2. Åtland, K. (2013). *The Security Implications of Climate Change in the Arctic Ocean*. In P. A. Berkman & A. N. Vylegzhanin (Eds.), Environmental Security in the Arctic Ocean (pp. 205-216). Springer Netherlands. https://doi.org/10.1007/978-94-007-4713-5_20, retrieved on 5 September 2020.
3. Buzan, B., Wæver, O., & Wilde, J. de. (2011). *Securitatea: Un nou cadru de analiză* (G. Jiglău, Ed.). CA Publishing.
4. Cățoi, I.-A. (2014). *Calea Maritimă de Nord*. Geopolitics.Ro. http://geopolitics.ro/calea-maritima-de-nord/, retrieved on 10 September 2020.
5. Corell, R. W. (2006). *Challenges of Climate Change: An Arctic Perspective. AMBIO: A Journal of the Human Environment*, 35(4), 148-152. https://doi.org/10.1579/0044-7447(2006)35[148:COCCAA]2.0.CO;2, retrieved on 20 September 2020.
6. Dăianu, D. (2015). *Cum să citim sancțiunile*. In *Marele impas în Europa: Ce poate face România?* (pp. 247-248). Polirom.
7. Garnett, S. (2008). *Russia's Illusory Ambitions*. In S. Secrieru (Ed.), *Rusia după Imperiu* (pp. 53-54). Institutul European.
8. Ghimiș, A.-M. (2011). *Cursa pentru Arctic*. Geopolitics.Ro. http://geopolitics.ro/cursa-pentru-arctic/, retrieved on 15 October 2020.
9. Ghimiș, A.-M. (2013). *Rim versus Non-Rim States in the Arctic Region: Prospects for a Zero-Sum Game or a Win-Win One?* In *Romanian Journal of European Affairs*, 13(3), 36-49.
10. Kaviani, R. (2017). *The Concept of Power in International Relations*. In *International Journal of Political Science*, 7(2), 29-36.
11. Keohane, R., & Nye, J. S. (2009). *Independența în politica mondială*. In *Putere și interdependență* (pp. 49-66). Polirom.
12. Koh Collin, S. L. (2020). *China's strategic interest in the Arctic goes beyond economics*. Defense News. https://www.defensenews.com/opinion/commentary/2020/05/11/

chinas-strategic-interest-in-the-arctic-goes-beyond-economics/, retrieved on 5 October 2020.

13. Krastev, I. (2014). *Russian Revisionism: Putin's Plan for Overturning the European Order*. Foreign Affairs. https://www.foreignaffairs.com/articles/russia-fsu/2014-03-03/russian-revisionism, retrieved on 5 October 2020.
14. Kristensen, H., & Korda, M. (2020). *Status of World Nuclear Forces*. FAS - Federation of American Scientists. https://fas.org/issues/nuclear-weapons/status-world-nuclear-forces/, retrieved on 5 October 2020.
15. Laverov, N., Lobkovsky, L., Dobretsov, N., & Vernikovsky, V. (2013). *Geodynamic model of the evolution of the Arctic basin and adjacent territories in the Mesozoic and Cenozoic and the outer limit of the Russian continental shelf*. Geoctonics, 47(1), 1-30.
16. Marshall, T. (2019a). *Arctica*. In *Prizonierii geografiei. Zece hărți care îți spun tot ce trebuie să știi despre politica globală* (p. 333). Litera.
17. Marshall, T. (2019b). *Rusia.* In *Prizonierii geografiei. Zece hărți care îți spun tot ce trebuie să știi despre politica globală* (pp. 29-30). Litera.
18. Morozov, V. (2015). *Russia in/and Europe: Source of Ambiguity*. In *Russia's Postcolonial Identity: A subaltern Empire in a Eurocentric World* (pp. 38-66). Palgrave.
19. Niemeschi, M. (2018). *Zone cu regimuri juridice internaționale speciale*. In Drept internațional public: curs pentru uzul studenților de la specializarea Relații Internaționale și Studii Europene (pp. 179-183). Hamangiu.
20. No More Pencils. (2018). *The GIUK Gap*. https://www.nomorepencils.com/giuk-gap/, retrieved on 15 October 2020.
21. Østhagen, A. (2019). *The Different Levels of Geopolitics of the Arctic*. Georgetown Journal of International Affairs. https://gjia.georgetown.edu/2019/12/05/different-levels-of-arctic-geopolitics/, retrieved on 15 October 2020.
22. Șișcanu, C. (2015). *Rusia legiferează explorarea Oceanului Arctic*. The Romanian Institute for the Study of the Asia-Pacific. http://risap.ro/rusia-legifereaza-explorarea-oceanului-arctic/, retrieved on 15 October 2020.
23. *The State Council of The People's Republic of China*. (2018). China's Arctic Policy. The State Council Information Office of the People's Republic of China. http://english.www.gov.cn/archive/white_paper/2018/01/26/content_281476026660336.htm, retrieved on 15 October 2020.
24. United States Environmental Protection Agency. (2016). *Climate Change and Extreme Heat: What You Can Do to Prepare*. https://www.epa.gov/sites/production/files/2016-10/documents/extreme-heat-guidebook.pdf, retrieved on 15 October 2020.
25. US Department of Defence. (2019). *2019 Department of Defence Strategy*. Office of the Under Secretary of Defense for Policy. https://media.defense.gov/2019/Jun/06/2002141657/-1/-1/1/2019-DOD-ARCTIC-STRATEGY.PDF, retrieved on 5 October 2020.
26. Yun, S. (2020). *Defining the Chinese Threat in the Arctic*. The Arctic Institute. https://www.thearcticinstitute.org/defining-the-chinese-threat-in-the-arctic/, retrieved on 5 October 2020.
27. Zodian, M. (2013). *Proliferarea armelor de distrugere în masă*. In *Relațiile Internaționale Contemporane*. *Teme centrale în politica mondială.* (pp. 117–133). Polirom.
28. Интерфакс. (2016). *В России появилась 45-я армия ВВС и ПВО Северного флота*. https://www.interfax.ru/russia/492208, retrieved on 5 October 2020.

THE MERITS AND LIMITATIONS OF MEMOIRS IN THE INTELLIGENCE FIELD: AN ASSESSMENT OF TRUTH AND DECEPTION PRESENT IN KIM PHILBY'S BOOK – *"MY SILENT WAR"*

Alin DREPTATE

Master degree graduate in Intelligence and Security Studies, Salford University, UK

This research supports the importance of memoirs with their merits and limitations, exemplified through the writings of a British double agent, Kim Philby. Philby's book, first published over fifty years ago, is a propagandistic material, portraying favourably the Soviet intelligence services. However, the memoir also presents embarrassing truths about questionable practices and failures of the British Secret Intelligence Service (SIS), highly likely never to be officially admitted. This article argues that memoirs are valuable and relevant as supplement of the archival evidence, pending on the ability to separate between truth and falsehood.

Keywords: memoirs; intelligence; espionage; deception; propaganda;

INTRODUCTION: A CRITICAL REVIEW OF THE MERITS AND LIMITATIONS OF MEMOIRS

Memoirs represent a relevant source of information, as they *"stand as historical sources both of the past they describe, and the present in which they were written"* (Haire, 2014, p. 777). A critical review of memoirs shows they present both merits and limitations, and understanding both of these aspects can enhance the quality of a piece of research, particularly when the official records are still too sensitive to be declassified. This first part of the article will first look at the merits followed by the limitations of using memoirs, and it will conclude with an assessment of the value of memoirs.

Memoirs are *"a vital way of supplementing archival evidence"* (Haire, 2014, p. 758) with their qualities *"of overcoming a shortage of contemporaneous sources"* (Ibid.) and offering *"insights into the attitudes and motivations of participants"* (Ibid.). Memoirs are important as they give *"a unique insight into the way individuals defined themselves and understood themselves"* (Popkin, 2017, p. 25). Ignorance of the cause of betrayal within a traitor's personality led to Robert Hanson being portrayed as *"a mediocre FBI agent"* (Muszynski, 2005, p. 221) and Aldrich Ames *"an under-achieving alcoholic"* (Ibid.), perspectives which were biased, superficial and one-sided. Similarly, Guy Burgess was described as a *"promiscuous man with twin vices: a bottle of gin and a book on flagellation"* (Lownie, 2015). Such shallow categorisations can be avoided by acknowledging a memoir's worth in describing *"personal and cultural aspects which are often especially well illuminated"* (Haire, 2014, p. 758), and because they cover the *"mentality and values"* (Tosh and Lang, 2006, pp. 64-65) and offer *"a fresh perspective and insight into the life of the <other>"* (Bacon, 2017, p. 389). Memoirs *"reveal one's character, basic values, and philosophy of life"* (Richman, 2006, p. 373), and therefore, their main quality is that they will offer the knowledge to understand the inherent *"self-justificatory element"* (Glynn and Booth, 1979, pp. 303-315), which is mostly absent or misjudged in official documents.

An additional merit of memoirs is that they *"are usable primary sources where the authors [write] from first-hand experience"* (Davies, 2001, p. 77), especially when *"the credibility of a source increases in direct proportion to the proximity of the source to its subject"* (Kerr, 1996, p. 566). The author's level of access allows researchers a better perspective of the event, particularly if the author of the memoir is *"a head of station reporting his unit's organisation"* (Davies, 2001, p.77). In this case it would make his or her statements *"the recollections of an insider' and more reliable when compared with redacted and scarce official records"* (Tosh and Lang, 2006, pp. 64-65). Such memoirs have the advantage of illustrating *"the practicalities and intricacies of intelligence relations"* (Haire, 2001, p. 774), which otherwise would be lost, or remained buried in a classified archive. Therefore, the placement and access of a memoir's author makes the memoir a valuable primary source of information.

Furthermore, memoirs may present a different perspective on the official version of the facts, which would be omitted or underrated according to the official policy of the government. When it comes to sensitive topics, the trend of authorities is to present the *"politically correct"* version of the facts, avoiding to present debatable information from human rights or moral perspective. Hughes et al. (2008) highlight the fact that *"official records, like all other records, are written for a purpose (and declassified or withheld for a purpose)"* (p. 14). This makes records of activities *"against allies […] more likely to be destroyed after use, weeded later or at least withheld from declassification for extraordinary lengths of time"* (Alexander, 1998, p. 2). Churchill's memoirs were vetted *"usually twice or three times"* (Reynolds, 2005, p. 211) to excise *"Churchill's ruder remarks about men such as Eisenhower, Tito and de Gaulle who had become significant [post-war] leaders"* (Ibid.). Hughes and Scott also remark that *"while the CIA has adopted a relatively liberal declassification policy in the United States, the archives of the British Secret Intelligence Service (SIS) remain effectively closed to researchers"* (Hughes et al., 2008, p. 5). Considering that this assertion remains true, memoirs are one of the few sources that can shed some light on these well-preserved secrets.

Memoirs become most valuable when studied in *"a triangulation triad"* form, along with *"primary sources (interviews, published first-hand accounts; and documentary sources – published or archival)"*. (Davies, 2001, p. 78). Such a comprehensive approach is highly recommended when the topic involves analysis of an intelligence matter between contradictory and competing accounts, as seen for example in two historically rival nations, such as the UK and France. Haire (2014) warns that *"it would be unwise to attempt to write about the Anglo-French intelligence relationship without examining some of the available memoir material in conjunction with archival evidence"* (Haire, 2014, p. 760), especially when a "memoir perhaps yields the best account of an event that can be traced" (Ibid.). Corroborating sources becomes significant when it comes to forgotten history where *"the personal narratives of those who have been involved in intelligence can and must be explored"* (Haire, 2014, p. 763), as they offer *"emotional and personal side of important relationships"* (Ibid., p. 760). Consequently, regardless of the time passed between the event and the writing of the memoir, the latter, by comparison with other sources of information, becomes *"a published artefact [which] is less volatile over time than memory, and hence possibly marginally more reliable"* (Davies, 2001, p. 77).

The memoirs have also shortcomings, as they can *"be deemed too unreliable for exclusive use"* (Hair, 2014, p. 776), when there is no primary or documentary sources to support them. When used as singular sources they serve *"as a record of events"*, [which] *"are often inaccurate and selective to the point of distortion"* (Tosh and Lang, 2006, pp. 64-65). The inaccuracy encompasses the *"subjective"*, with the recall of facts based on an *"arbitrary timeframe of the individual life and the perspective of the individual"* (Hair, 2014, p. 761). Memories suffer changes due to the *"choices which memories to include and how to portray them"*, and present a retrospective view of what seemed important combined with an emotional *"remodelling"* (Bacon, 2017, p. 389). Memoirs have similar flaws to autobiographies and *"are heavily dependent on the autobiographer's very ability to remember"* (Summa-Knoop, 2017, p. 3). Considering that *"not all alterations and not all distortions qualify as lies"*, the information can poorly mirror the reality, with the same event being recalled differently by multiple individuals (Bacon, 2017, p. 389). The intentional alteration of memories take place because memoirs involve *"personal narratives"* (Hynes, 1999, pp. 205-220), which suggests that those who write them are *"makers"* (Ibid.). The memoir's faithfulness to the truth suffers because of the individuals' intentions *"to exonerate themselves, elevate their positions, or to applaud or condemn the institutions they examined"* (Haire, 2014, p. 763). The latter case was seen in Compton Mackenzie's Water on the Brain, where *"he wickedly mocked SIS and its management"* (West, 2004, p. 278). Additionally, the exposure to external factors (such as manipulation of data to serve the targeted audiences) supports the claim that the *"production of a memoir or autobiography is arguably as social an activity as conversation"* (Haire, 2014, p. 763). With such limitations, it is difficult to evaluate and differentiate to what extent the intentional or unintentional distortion took place and how it manipulated the truth described in a memoir.

Another disadvantage is that memoirs are an account of the author's life and less a *"historical truth"* (Haire, 2014, p. 763), which may describe events in a *"revelatory and provocative style"* (Defty, 1995, p. 184). Exaggeration is used as an attempt to maintain the interest of the reader, while concealing or compensating for areas when the historical perspective of an account is filled *"with such vagueness that it is impossible to verify"* (Haire, 2014, p. 772) or to provide details. The *"varying degrees of self-censorship"* (Defty, 1995, p. 184) create difficulties for the historian in *“the extraction of facts from sensationalism”* (Ibid.), which led for example the British intelligence community to be known in its early days *“in the form of memoirs, fictionalised memoirs and classic spy fiction”* (West, 2004, p. 276). Such limitations led Defty to state that *“the British intelligence memoir, like all memoirs, must be read with some care”* (Defty, 1995, p. 184). The degree of sensationalism and oversimplification can make memoirs a source of disinformation, contributing to either “intelligence literature lies”, or at least to increased difficulty in determining the accuracy of the intelligence-related work (West, 2004, p. 279). Sensationalised or oversimplified memoirs are seen in democratic states, where the stories *“are decidedly patchy and at times quite vague”* (Defty, 1995, p. 186), but also in autocratic states. In the latter, the authors *“typically have an agenda of disinformation or self-aggrandizement”* (Muszynski, 2005, p. 220) or write *“to berate the services for their actions both during and since their employment”* (Defty, 1995, p. 184). As a result, memoirs can suffer in accuracy due to author’s attempt to make the book more commercial or to gratify the service or the state he or she serves.

In conclusion, the use of memoirs must be done with caution and careful handling can offer benefits and enhance the quality of research. When it comes to intelligence, every piece of information is valuable, regardless of whether it is true or not, because in the first case it augments the current historical facts, while in the second one, it demonstrates the intention of deceiving. Most successful deceptions are not fully-fledged falsehood, but a combination of truth and lies which allows, under a rigours screening, a separation between the two. Memoirs, despite their drawbacks in being subjective and malleable under their writer’s pen, supplement the archival evidence, can offer first-hand information, and when used in corroboration with other materials can exceed the value of official records.

A DEFECTOR’S MEMOIR: AN ASSESSMENT OF TRUTH AND DECEPTION PRESENT IN KIM PHILBY’S BOOK – *“MY SILENT WAR”*

Kim Philby’s memoir is a controversial source of information about the British and American intelligence services’ activities during the Second World War and the Cold War, and it fuses elements of truth with disinformation and propaganda. This part of the article will first analyse the information assessed as true, followed by an inquiry into the deceptive messages present in Philby’s book, in both cases cross-checking his memoir with archival evidence and secondary sources. The study will attempt to assess the veracity of Philby’s accounts of several cases presented in his memoir, and whether it can be used as a reliable source to augment the existing information on intelligence-related activities during the Second World War and the Cold War.

The memoir truthfully highlights the difficulties of cooperation between Britain’s Security Service (MI5) and the Secret Intelligence Service (SIS/MI6) *“due to basic differences of opinion about the line of jurisdictional demarcation between the two organisations”* (Philby, 2018, p. 43) and *“personal factors”* (Ibid.). Both MI5 and Section V of MI6 had overlapping responsibilities in counter-espionage, and despite the fact that the first organisation was focused on *“foreign territory”*, while the second was supposed to concentrate on British territory, conflicts between the two still emerged (Harrison, 1995, p. 522). Regardless of Philby’s personal agenda to *“attempt to vilify MI5”*, he correctly observed the strains between the two services, and his assessment is supported by other accounts (Harrison, 1995, p. 514). The two services *“quarrelled over the control of agents”* (Harrison, 1995, p. 522), and the Security Service *“found SIS neither helpful nor efficient”* (Ibid.). When it came to countering espionage, MI5 was *“unsatisfied”* (Harrison, 1995, p. 523) and “found the SIS performance of its Counter-Espionage duties inadequate” (Ibid.). The complaints came also because SIS delayed *“in reporting the facts”* following the Ultra intercepts about two major operations, Garbo and Tricycle (Harrison, 1995, p. 523). These corroborated testimonies support the assessment that Philby’s memoir presents truths that are valuable in establishing historical facts and which are sometimes concealed or distorted even by official documents.

As argued in the previous paragraph, during the Second World War cooperation between British intelligence services was poor, and this was partly attributed to the SIS leadership. Philby’s memoir brought into debate the low-level of professionalism of SIS leaders, such as the SIS chief, Major General Sir Stewart Menzies and Felix Cowgill, Section V’s chief, together with other SIS personnel. Menzies’ intellect *“was unimpressive”*, having the knowledge only of a “fairly cloistered son of the upper levels of the British Establishment” (Philby, 2018, p. 109) and, according to Philby, his counterintelligence training was reduced to *“schoolboyish-bar, beards and blondes” (Ibid.) attitudes. Other authors corroborate this description, with Menzies labelled as “not suitable as a Chief of the Secret Intelligence Service”* (Harrison, 1995, p. 515) and *“not a very strong man and not a very intelligent one”* (Howarth, 1986, p. 115) who *“drew his personal advisers from a painfully limited social circle”* (Trevor-Roper, 1968, p. 72). This assessment is augmented by Christopher Andrew’s remark that the MI6 leadership during wartime *“was not of the calibre of some of the senior professionals in MI5 and GC & CS”* (Andrew, 1985, p. 462). Similarly, Section V chief Felix Cowgill’s *“intellectual endowment was slender”* (Philby, 2018, p. 55) and his professional skills were *“inhibited by lack of imagination, inattention to detail and sheer ignorance of the world we were fighting in”* (Ibid.), combined with a tendency for *“self-destruction”* (Ibid., p. 97). Cowgill was also accused of having *“stood by his own staff far beyond the call of loyalty, retaining* *many long after their idleness or incompetence had been proved"* (Philby, 2018, p. 46). Despite the tribute from Robert Cecil that *"Section V had rapidly expanded and continued to do so under Cowgill's direction"* (Cecil, 1994, p. 765), Ben Macintyre confirms in his book Philby's perspective on Cowgill's lack of professionalism, and characterises him as *"rigid, combative, paranoid and quite dim"* (Macintyre, 2014, p. 27). When evaluating the quality of other SIS personnel, the latter showed little professionalism: *"He (Philby) is plum right about Vivian and Dansey. Vivian was a nice wet man with no guts...Dansey was a snobbish, arrogant, incompetent shit and I've never met anyone who disputed it"* (Harrison, 1995, p. 516). Harrison also supports the evaluation that the *"SIS grass-roots personnel were of mixed quality"* (p. 516) and he quotes Lord Dacre's description of SIS as *"by and large pretty stupid and some of them very stupid"* (Ibid.). All these testimonies support the argument that despite some of Philby's biases towards certain powerful figures within MI5, which led him to spread false information about them, his account of the SIS leadership is truthful, and explains some of the MI6 failures which have been attributed to poor leadership.

Throughout the memoir, Philby illustrates SIS's value between 1940 and 1946 by labelling it as *"of mythical prestige"* (Philby, 2018, p. 22) with *"little substance"* (Ibid.), and stating that *"if the British genius leans towards improvisation, then SIS is a true reflection of it"* (Ibid., p. 41). The memoir correctly underlines the limited success and professionalism of Section D within SIS, starting with its staffing organigram *"if it had one"* (Philby, 2018, p. 12), and stressing the *"disparity between ends and means"* (Ibid.) and their *"slender resources"* (Ibid.). Philby ridiculed his colleagues at Section D who intended to destroy the Iron Gates of the Danube, as, in his opinion, they equated this operation with *"destroying the pintle of a lock-gate in the Regent's canal"* (Philby, 2018, p. 12), and which eventually resulted in causing the British government "some embarrassment" (Ibid.). Harrison confirms Section D's inefficiency during the Second World War with two other failed sabotage attempts, one *"to block the Danube by blowing up a cliff"*, and a second to disrupt Swedish iron ore production, the latter resulting in one SIS officer being arrested and another one fleeing (Harrison, 1995, p. 514). The performance of SIS's human intelligence collection was similar to that of Section D. Philby mentioned the complaints of *"three service Directors of Intelligence (DI)"* (Philby, 2018, p. 110), members of the Joint Intelligence Committee, because *"secret intelligence obtained by SIS was inadequate"* (Ibid.) and he confirmed the three DIs had *"some substance in their allegations"* (Ibid.). Other assessments of SIS's wartime activities avowed that SIS *"agent information produced nothing of value throughout the war"* (Harrison, 1995, p. 517) and their information was *"routinely disbelieved by intelligence staffs"* (Ibid.). In other situations when it was acted upon it, it resulted

in *"disasters"* (Ibid.). The SIS analysis department also failed to predict the German annexation of Austria in March 1938, the German occupation of Czechoslovakia in March 1939 and the invasion of Holland. The effect of those failures was that in 1940 SIS had reduced capabilities, and this resulted in the arrest of the SIS Vienna station chief, *"the collapse of the SIS network in Czechoslovakia"* (Ibid., p. 518) and the closure of *"the SIS stations in Oslo, Copenhagen, Paris, Rome, Brussels and The Hague"* (Ibid.). All these elements support the assessment that Philby's memoir does provide pieces of information which can reliably be corroborated with other primary and secondary sources. Such corroboration provides a more accurate picture of the reality during wartime, despite the general reservations associated with using memoirs as a valid source of information.

The next section to analyse is Philby's inside information about the internal struggles within SIS, which clarifies some of the circumstances surrounding the dismissal of Felix Cowgill as a potential Section IX chief. In this case, Philby arranged for the removal of Cowgill *"with surgical detachment, and no remorse"* (Macintyre, 2014, p. 91) by exploiting his role as *"an antagonist in inter-office strife"* with MI5 (Philby, 2018, p. 98). Philby's master plan included *"no overt measures"* (Philby, 2018, p. 94) against Cowgill, with *"every move in the campaign (…) [coming] from someone else"* (Ibid.) and using allies found *"in the ranks of Cowgill's enemies"* (Ibid.). Describing the steps Philby used to achieve his goal shows that memoirs provide valuable pieces of information to complement the facts already known, in this case, the appointments to MI6 lead positions. Additionally, the internal SIS conflicts and the lack of released archival documents in regard to this matter make Philby's confession a relevant contextual document which permits the identification of the security system's vulnerability in the form of informal networking and lobbying to appoint MI6 sections' leaders.

In addition to inside information about the SIS, Philby's memoir provides information about other British intelligence services' activities. One such activity was the opening of the diplomatic bags of allied nations during the war, a highly questionable activity and one unlikely to ever be admitted by government officials. Philby mentions that *"the bags of neutral states and of minor allies, such as the Poles and the Czechs, were fair game"* (Philby, 2018, p. 51) and the diplomatic correspondence of others *"was regularly subjected to scrutiny"* (Ibid., p. 53). Philby described the procedure in detail and gave the example of one case when *"the red seals in a Polish bag turned purple under treatment, and nothing could be done to restore them"* (Philby, 2018, p. 53). The opening of diplomatic bags of allied nations which transited British territory is surprising in the case of Poles, especially when British intelligence worked in close cooperation with them and were dependent on the Poles' *"extensive network of informers in Europe"* (Harrison, 1995, p. 519). However, considering the clandestine opening of diplomatic bags a regular non-technical information collection tactic performed by every intelligence service which had the capability and the will to assume the risk, it is highly likely that Philby is telling the truth about the matter (Herman, 1996, p. 79). Despite Philby's questionable motives for reporting this practice, the opening of diplomatic bags confirms other available information on the customary practices of intelligence services in times of conflict, subsequently making the memoir a corroborative source on questionable wartime practices.

When discussing several MI6 operations, the memoir provides context to some of them, and an example is seen in the case of the Russian vice-consul in Turkey, Konstantin Volkov. After realising the value of the information that Volkov was willing to offer, Philby realised that his friends, Guy Burgess and Donald Mclean, and even he, were at risk of being exposed as Soviet informers (FCO 158/57, 1952, p. 140). Volkov allegedly knew the identities of *"three Soviet agents working in Britain. Two of them were in the Foreign Office; one was head of counter-espionage organisation in London"* (Philby, 2018, p. 119), details which matched three members of the Cambridge Five spy ring (FCO 158/57, 1952, p. 251). Philby admitted in his memoir that his delayed arrival in Turkey to debrief Volkov would work in his favour and acted accordingly by arriving as late as possible. When he was challenged about why he arrived nearly three weeks later in Turkey after Volkov first contacted British representatives, he replied that any change in his schedule *"would have interfered with leave arrangements"* (Macintyre, 2014, p. 101). John Leigh Reed corroborates Philby's late arrival by considering his delay at that time as *"just irresponsible and incompetent"*, facts which eventually led to Volkov and his wife being taken back to Russia and highly likely executed (Ibid.). Despite the fact that the context of this case is described only vaguely, at least Philby brings a perspective which is missing from released official archives.

In the case of Volkov's *"disappearance"*, Philby concealed information and forwarded the hypothesis that because of the *"nearly three weeks"* (Philby, 2018, p. 127) between first approach and his attempt to contact him, *"the Russians had ample chances of getting on to him"* (Ibid.). Philby did not officially acknowledge he was the one who had sentenced Volkov to death and presented his theory that Volkov and his *"insistence on bag communications had brought about his downfall"* (Philby, 2018, p. 119). Moreover, despite the fact that it was known that Volkov *"was forcibly abducted from Istanbul a few days before Philby arrived [in Turkey]"* (Cecil, 1994, p. 766), the idea that the Russians were tipped off had *"no solid evidence to support it"* (Philby, 2018, p. 128). Philby acknowledged his role in this affair only later, when, following a meeting in Moscow with Phillip Knightley, he was quoted as considering Volkov's case *"a nasty piece of work"* (Knightley, 1988,

p. 138), and saying that the Russian *"deserved what he got"* (Ibid.). In this case, while official records show Philby's travel itinerary to Turkey and the outcome in regard to this case, Philby's memoir exposes some of the deception he used. Philby omits relevant pieces of information about the case and attempts to present the reader a hypothesis which absolves him of any guilt, tactics consistent with Soviet's disinformation strategy to deny the crimes and to blame the victim for the negative outcome.

Notwithstanding the depictions of certain true facts, Philby's memoir is likewise a work of propaganda and a disinformation instrument sanctioned and promoted by the KGB. Kim used his *"duplicity and charm"* (Philby, 2018, p. xv) in the *"pursuit of his long vendetta against the West in general and, in particular, against the British and American intelligence communities"* (Cecil, 1994, p. 764). Kim's deceptions in his memoir started with claims of not *"incurring the charge of wanting to muddy waters"* (Philby, 2018, p. xxvi) and trying *"simply to correct certain inaccuracies and errors of interpretation"* (Ibid.). His mastery in deception is present from the early pages of his book, when he caveats his thoughts against any criticism by claiming that *"this book is not a history or a treatise or a polemic. It is a personal record"* (Philby, 2018, p. xxx). He continues by stating his duty to answer questions *"even if the answer takes the form of gross over-simplification"* (Philby, 2018, p. xxxi). However, his intellect *"as sharp as a cut-throat razor"* (Ibid. p. ix) *"succeeded in poisoning the well"* (Cecil, 1994, 765) by convincing Graham Greene, who, in line with his dubious motivation, labelled the book a *"honest"* account, with no propagandistic messages and a *"dignified statement of his [Philby's] beliefs"* (Philby, 2018, p. xvii). In obvious contradiction to this, Philby's memoir is *"a brilliant piece of propaganda"* (Harrison, 1995, p. 514), *"an expression of his <cover personality>"* (Cecil, 1994, p. 764), and there are at least *"14 cases where Philby lied, distorted the facts, or omitted major episodes"* (Harrison, 1995, p. 515). Overall, the deception and propaganda in his book, in the form of outright lies, mixed truth and fabrications, or withheld information, is destined to protect the image of the service he always worked for, the KGB.

In line with his deception, Philby portrays himself as more than a traitor and eulogizes his recruitment and his communist allegiance in opposition to his presumed natural loyalty to the UK and the SIS. Despite the fact that the Russians considered him *"agent Tom"* until his death, following *"his easy escape from Beirut [which] invited suspicion he was still working for the British government"* (Cecil, 1994, p. 765), *"in early manhood"* (Coffey, 2015, p. 43) he called himself *"an accredited member of the Soviet intelligence service"* (Philby, 2018, p. xxviii). Also, after the Spanish civil war, he valued himself *"as a fully-fledged officer of the Soviet service"* (Philby, 2018, p. xxx). He justified his KGB recruitment by stating that *"one does not look twice at an offer of enrolment in an elite force"* (Philby, 2018, p. xxxii). Such a force had only been in existence for 16 years by1934 (the year of Philby's recruitment), and it was part of a system where ideology was more important than professionalism, as demonstrated by Joseph Stalin's purges, making it unlikely that the force was *"elite"*. Also, Philby's ideological perspective was aligned with Communist messaging against Nazism, but he totally disregarded inconvenient truths, such as the fact *"that until Hitler invaded USSR on 22 June 1941 Communist parties not only refused to oppose him, but on orders from Moscow actively co-operated with him"* (Cecil, 1994, p. 765). Furthermore, his positions within the SIS were nothing more than *"cover jobs"* (Philby, 2018, p. xxix) to better serve the Soviet Union, which was *"the inner fortress of the world movement"* (Ibid.). In Philby's faulty belief, if it was not for *"the Soviet Union and the Communist idea, the Old World, if not the whole world, would now be ruled by Hitler and Hirohito"* (Philby, 2018, p. xxxii). These assertions make it clear without a doubt that Philby's memoir is more than a personal account and contains a political and ideological message, and not surprisingly his message does not reflect reality.

Turning the attention to particular incidents, the memoir omits the details of events in which Philby was involved, mostly in cases that were morally questionable or challenged the infallible communist ideology. During his assignment in 1937 during the Spanish Civil War, despite Philby's declared mission *"to get first-hand information on all aspects of the Fascist war effort"* (Philby, 2018, p. 3), he omits to mention that his presence there *"was to organise the murder of General Franco"* FCO/27, 1952, p. 251). A similar example is seen when Philby talks about *"General Krivitsky, the Red Army intelligence officer who defected to the West in 1937, only to kill himself a few years later in the United States – a disillusioned man"* (Philby, 2018, p. 105). Philby outright disregards any chance of him having been murdered by NKVD, *"although evidence suggests an operation by Soviet <hitmen>"* (Cecil, 1994, p. 766). These examples show that in cases when Philby was involved in questionable operations, such as facilitating assassinations, or when it exposed the true oppressive trait of communism, the memoir does not mention the actual details of the episode.

Other examples of actions omitted from the memoir include Philby's providing Russian intelligence with the names of people opposed to the Soviet agenda who would become leaders within their countries (back then under Soviet influence). These people opposed the USSR's plans to *"take-over of the countries concerned, regardless of the wishes of the inhabitants"* (Cecil, 1994, p. 766). Philby omits to mention in his memoir that he *"shared with the Soviets the names of leading Catholics in Germany who could play a role in government after the war. The Kremlin had many of them killed or imprisoned"* (Coffey, 2015, pp. 42-43). Also, Philby's' role in crushing the insurgency in Albania is not mentioned, and according to him *"the operation was quietly dropped without having made any noticeable dent on the regime in Tirana"* (Philby, 2018, p. 156) because British and American governments' *"squib proved so damp"* (Ibid.). However, in reality the Albanian operation (mostly between 1949-1951) failed so categorically because Philby *"gave away plans of the United States and Britain to infiltrate insurgents into Albania, thus ensuring these raiding parties were all rolled up"* (Coffey, 2015, pp. 42-43). Therefore, the facts which would have shown the imposition of Communism in certain countries as the result of the USSR's intervention and not as the will of the people were removed from the memoir, and the US and the UK were blamed for their *"imperialistic"* ambitions.

CONCLUSIONS

Philby's memoir combines true and distorted facts to give his book more credit, either to promote it as a historical document or for it to serve as a propaganda tool for those who might want to adhere to the communist ideology or to betray their countries. The memoir starts as a confession where Philby justifies the path he chose and offers valuable insight into why he became a source of information for Russian intelligence. When he discusses the circumstances of his work in the SIS, his relationship with MI5 or the cooperation with the US intelligence community, Philby's memoir mixes truth and false statements. Philby wrote his memoir in this way highly likely following a NKVD editing process or as the consequence of his grudges towards certain individuals, in either situation promoting false information. His memoir becomes more untrustworthy when he reaches morally challenging circumstances in regard to how some of his actions will be perceived by the public, or to actions which could compromise the image of Communist ideology. On these occasions, his memoir omits details, alters parts of the information presented or simply falsifies the facts. In these instances, establishing the truth becomes a matter of prediction, following the lack of a *"standard against which Philby's narrative could be judged"*, and with a degree of certainty based on accounts of other actors present during that time (Cecil, 1994, p. 767). Reasons such as *"the enforced silence of the intelligence community"* (Ibid.) or the fact that *"successive governments refused to provide authentic accounts"* (Ibid.) only manage to augment Philby's side of the story, and 52 years later facts and questions remain debated and unanswered. Despite all these drawbacks, Philby's memoir, used with caution, increases the amount of information available and has triggered responses from other intelligence professionals, aspects which have enriched the intelligence community's knowledge about intelligence during and after the Second World War.

BIBLIOGRAPHY:

1. Alexander, S.M. (1998). *Introduction: Knowing Your Friends, Assessing Your Allies – Perspectives on Intra-Alliance Intelligence.* Intelligence and National Security 13(1).
2. Andrew, C. (1985). *Secret Service: The Making of the British Intelligence Community*. London: Guild Publishing.
3. Idem, (2018). *Russia active measures under Putin – a long term perspective*. Study *Group on Intelligence-King's College and Cambridge Intelligence Seminar*. London.
4. Bacon, E. (2017). *The scholarly exegesis as a memoir*. New Writing, 14(3).
5. Cecil, R. (1994). *Philby's Spurious War*. Intelligence and National Security, 9(4).
6. Coffey, T.G. (rev.) (2015). *Intelligence in Public Literature*. Studies in Intelligence 59(1).
7. Compton, M. (1932). *Greek Memories*. London: Cassell.
8. Idem, (1933). *Water on the Brain*. London: Chatto&Windus.
9. Davies, H.J.P. (2001). *Spies as Informants: Triangulation and the Interpretation of Elite Interview Data in the Study of the Intelligence and Security Services*. Politics, 21(1).
10. Defty, A. (1995). *The future of the British intelligence memoir* (Review Article), Intelligence and National Security, 10(1).
11. Denniston, R. (1992). *Three Kinds of Hero: Publishing the Memoirs of Secret Intelligence People*, *Intelligence and National Security* 7(2).
12. Di Summa-Knoop, L. (2017). *Critical autobiography: a new genre?*, Journal of Aesthetics & Culture.
13. Glynn, S., Booth, A. (1979). *The Public Records Office and Recent British Economic Historiography*, The Economic History Review 32(3).
14. Haire, E.J. (2014). *A Debased Currency? Using Memoir Material in the Study of Anglo-French Intelligence Liaison*, *Intelligence and National Security*, 29(5).
15. Harrison, E.D.R. (1995). *More thoughts on Kim Philby's My Silent War, Intelligence and National Security*, 10(3).
16. Herman, M. (2003). *Intelligence power in peace and war*. Cambridge: Cambridge University Press.
17. Howarth, P. (1986). *Intelligence Chief Extraordinary: The Life of the Ninth Duke of Portland*. London: The Bodley Head.
18. Hughes, R.G., Jackson, P., Scott, L. (eds.) (2008). *Exploring Intelligence Archives: Enquiries into the Secret State*. London/New York: Routledge.
19. Hynes, S. (1999). *Personal Narratives and Commemoration in Jay Winter and Emmanuel Sivan* (eds.), *War and Remembrance in the Twentieth Century*. Cambridge: Cambridge University Press.
20. Kerr, S. (1996). *KGB sources on the Cambridge network of Soviet agents: True or false?, Intelligence and National Security,* 11(3).
21. Knightley, P. (1988). *Philby: KGB Masterspy*. London: Andre Deutsch Ltd.
22. Lownie, A. (2015). *The most promiscuous man who ever lived*, Daily Mail, https://www.dailymail.co.uk/news/article-3216458/The-promiscuous-man-lived-New-biography-Guy-Burgess-reveals-Cambridge-spy-sleep-17-75-real-passion-treachery.html, retrieved on 6 September 2020.
23. Macintyre, B. (2014). *A Spy Among Friends*. New York: Crown Publishers.

24. Modin, Y., Deniau, J.-Ch., Ziarek, A. (1994). *My five Cambridge friends*. London: Headline.
25. Muszynski, M. (2005). *Spy Handler: Memoir of a KGB Officer*, Journal of Military Ethics, 4(3).
26. Philby, K. (1981). *Briefing of East German intelligence service (STASI)*. BStU via Associated Press.
27. Idem (2018). *My silent war. The autobiography of a Spy*. London: Arrow Books.
28. Popkin, D.J. (2017). *History, Historians, and Autobiography Revisited*, a/b: Auto/Biography Studies, 32(3).
29. Reynolds, D. (2005). *The Ultra Secret and Churchill's War Memoirs. Intelligence and National Security*, 20(2).
30. Richman, S. (2006). *When the Analyst Writes a Memoir*, Contemporary Psychoanalysis, 42(3).
31. Tosh, J., Lang, S. (2006). *The Pursuit of History: Aims, Methods and New Directions in the Study of History*, 4th ed. Harlow: Pearson Longman.
32. Trevor-Roper, H. (1968). *The Philby Affair: Espionage, Treason, and Secret Services*. London: William Kimber.
33. Watt, D.C. (1988). *Intelligence Studies: The Emergence of the British School*. Intelligence and National Security 3(2).
34. West, N. (2004). *Fiction, Faction and Intelligence*. Intelligence & National Security, 19(2).
35. FCO 158/175, Guy Burgess, Donald Maclean: allegations that Kim Philby (Peach) was the 'third man',1 January1955-31 December 1955.
36. FCO 158/27, Kim Philby (Peach): file 1, 1 January 1951-31 December 1952.
37. KV 2/1603, Communists and suspected communists, including Russian and communist sympathizers: Alexander Ethan Tudor-Hart, alias Harold White: British, 1 January 1929-31 December 1943.
38. KV 2/4091, The Security Service: Personal (PF series) files. Edith Tudor-Hart, aliases Suschitsky, White, Betty Grey, codename Edith: Austrian, nationalised British, 24 October 1951-17 March 1952.
39. Soviet television/KGB, Comrade Philby. Interviews of former KGB officers case officers,14 May 1990, British Film Institute National Archive.

PERSPECTIVES ON ADAPTING MILITARY STRUCTURES TO THE REQUIREMENTS OF CURRENT AND FUTURE OPERATIONAL ENVIRONMENTS

Lieutenant-Colonel Assoc. Prof. Paul TUDORACHE, PhD

"Nicolae Bălcescu" Land Forces Academy, Sibiu

Colonel Assoc. Prof. Lucian ISPAS, PhD

"Nicolae Bălcescu" Land Forces Academy, Sibiu

Approaching the current and future operational environments requires that military structures and, in particular, the tactical ones, should have the ability to conduct operations, regardless of the campaign themes (peace military engagement, peace support operations, security operations, and combat operations), which involves the simultaneous or successive use of tactical activities and core functions in order to generate the desired effects and, implicitly, to attain the end state. In this regard, an operational adaptation of the tactical military structures is required, generating, at the same time, implications at the level of the force structure, not only by reconfiguring the organic headquarters (HQ), but also by reorganising the combat (CBT), combat support (CS) and combat service support (CSS) forces. Therefore, highlighting the specific aspects of the combat power's adaptation, by analyzing the established war fighting functions (WFF), the finality of the article will seek to identify the main adjustments of the military decision making process (MDMP), as a fundamental planning methodology used by tactical military structures, with organic staff.

Keywords: COE; FOE; operational adaptation; combat power; WFF;

INTRODUCTION. WHY AN OPERATIONAL ADAPTATION OF MILITARY STRUCTURES?

Nowadays, the approach of operational environments requires that commanders, military staffs (Headquarters – HQ) and subordinate forces should have the ability to continuously adapt, even within the same operation, involving successive operational changes in all phases of the operations process (planning, preparation, execution, assessment). This requirement is based on the lessons learned from recently completed or on-going military operations, such as Operation Inherent Resolve (OIR), whose common denominator was that the initial plan survived only in the early hours of execution, as what was anticipated in the planning did not correspond to the reality on the ground, because the conditions of the operational environments changed in relation to the dynamics of the combat actions.

Given these conditions, the following question arises: *"What are the characteristics of current and especially future operational environments that planners should take into account in the operations process?"*. The answer to this question is quite difficult, requiring a thorough analysis and interpretation of specialised sources.

In order to identify the reference characteristics of the operational environments we should first understand it from a holistic perspective. In this sense, the operational environment is defined by intelligence specialists as *"a mixture of conditions, circumstances and influences that affect the engagement of capabilities and decision-making by the commander"* (JP 3-0, 2017, p. IV-1). It also includes the following factors (JP 3-0, 2017, p. IV-1):

- physical areas – defined by the air, land, sea, space domains;
- information environment – includes cyberspace;
- electromagnetic spectrum (Electromagnetic Spectrum – EMS);
- other factors.

Analysing *figure 1*, it can be seen that within these factors the relationships between own forces, adverse, neutral or other interest audiences can be defined.

Relating all these factors *(figure 1)* to recent operational contexts such as those in Ukraine, Afghanistan, Syria, Iraq, etc. we can establish that they generated real difficulties in determining the specific parameters, because the operational

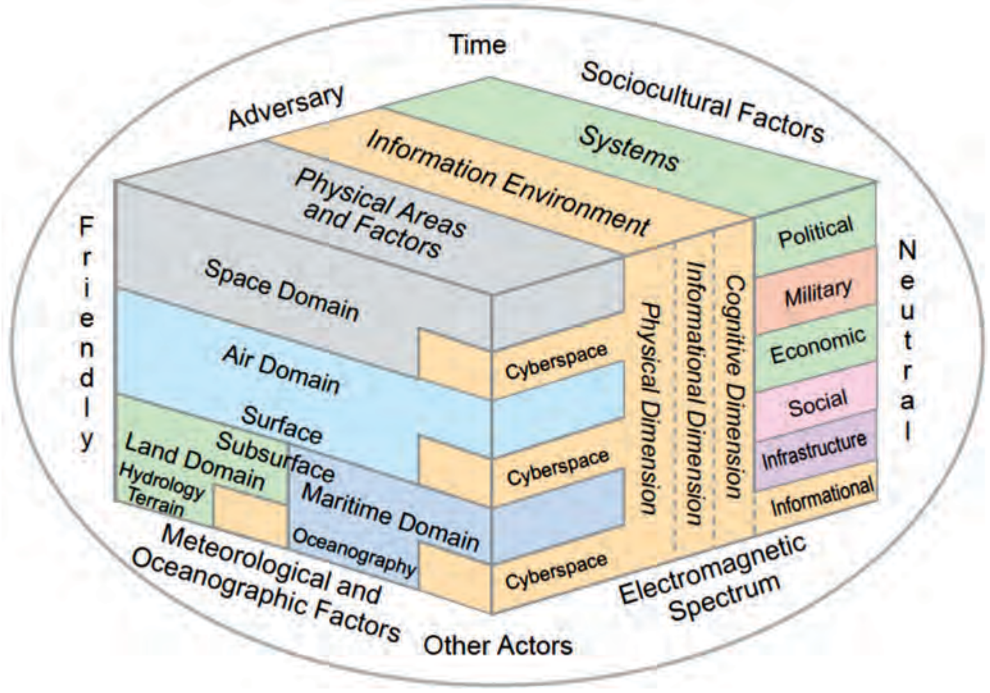


Figure 1: Physiognomy of the operational environment (JP 2-01.3, p. I-3)

environments were classified as volatile, uncertain, complex and ambiguous *(Volatility, Uncertainty, Complexity, Ambiguity – VUCA)*. Consequently, the current operational environments (COA) and especially the future ones *(Future Operational Environment – FOE)* will be characterised by (Karaoguz, 2016, p. 8):

- volatility – coagulated by the presence of instability in the operational environment/area of operations *(Area of Operations – AO)* from the perspective of information exchange and the specific of the situation;
- uncertainty – results from the difficulty of understanding the situations and the predictability of the effects generated as a result of the changes of the operational contexts;
- complexity – consists in the multitude of actors present in the operational environment, on the one hand, and on the other hand the manifestation of the confusion of problems, due to the difficulty of defining the relations between causes and effects;
- ambiguity – given by the lack of clarity in visualising and understanding the situational contexts (the principle action – reaction – counteraction) as a result of the erroneous definition of the *Common Operational Picture (COP)*.

Certainly, the visualization and understanding of the characteristics of COE/FOE are correlated with the time horizon, and on this principle it can be concluded: *the longer the time horizon of visualising the operational environments, the more pronounced the VUCA type characteristics will be*.

OPERATIONAL ADAPTATION – IMPERATIVE OF THE COE/FOE APPROACH

In order to identify the possibilities for the operational adaptation of military structures to the specific of the COE/FOE, we will start from the analysis of combat power, as there were operational contexts where friendly forces have faced difficulties in applying it at the right time and decisive place.

One of the most appropriate definitions given to combat power is *"the application of fighting power through warfighting functions"* (AJP 3.2, 2016, pp. 2-27), using *"leadership and information"* (Wade, 2015, pp. 1-22). By the way, information is used in the sense of exchanging information between their own structures, but also between them and other cooperation structures. The configuration of the combat power, used as a starting point in the process of adapting it, is highlighted in table 1.

Table 1: Elements of combat power

	+ leadership (multiplies and unifies the combat power elements)			
Combat power	WFF	*intelligence* allows understanding the enemy and all elements of the operational environment (ADP 3-0, 2019, p. 5-4)	*information activities* affects information systems, influencing the behavior of interest audiences (AJP 3.2, 2016, p. 2-16)	*movement and maneuvre* ensures the mobility and use of forces in order to obtain advantageous positions over the enemy (ADP 3-0, 2019, p. 5-3)
			command and control allows commander to synchronise and converge the elements of combat power (ADP 3-0, 2019, p. 5-3)	
		fires ensures the use of direct/indirect fires, air and missile defence and joint fires to engage targets (Wade, 2015, p. 1-23)	*sustainment* provides services of all classes in order to maintain and expand operational capacity (ADP 3-0, 2019, p. 5-5)	*protection* preserve the combat power necessary to fulfill specific missions (ADP 3-0, 2019, p. 5-6)
	+ information (understood as communication between structures)			

On the other hand, the adaptation of combat power should be correlated with the standards for the development of military capabilities to operate in the context of the COE/FOE, as follows:

- operational flexibility and mental agility of leaders;
- modularity and versatility of forces;
- strategic/operational deployment and tactical mobility of forces;
- the personnel's expeditionary mentality of the deployable structures;
- integration of Artificial Intelligence (AI) at the HQ level and CBT, CS, CSS forces.

Therefore, taking into account the VUCA-type characteristics of the COE/FOE and the standards of military capability development presented above, we will adapt the combat power, making adjustments at the level of each WFF, as follows:

- command and control (C_2) – should be applied in the sense of mission command in order to encourage disciplined initiative and freedom of action of subordinate leaders; in this way, commander and HQ will be able to perform specific tasks related to operational requiremets within COE/FOE (table 2).

Table 2: Mission command tasks (ADRP 6-0, pp. 1-4-1)

Primary tasks	
Commander tasks	**HQ tasks**
- drive the operations process by understanding, visualizing, describing, directing and assessing operations; - develop tems, not only within own structure, but also including joint, interagency, intergovernmental, multinational (*Joint, Interagency, Intergovernmental, Multinational – JIIM*) parteners; - inform and influence the audiences inside/outside their structures.	- conduct the operations process including planning, coordination, execution and assessment; - conduct the management of knowledge and information; - conduct inform/influnce activities; - conduct cyber electromagnetic activities.
Additional tasks (driven by commander and conducted by HQ)	
- drive/conduct deception operations; - drive/conduct engagement operations (pointed to local population); - intal/operate/maintain C_2 network; - drive/conduct airspace control; - drive/conduct information protection.	

- intelligence and information activities – merged in a single WFF, will generate an accentuated active character by using the intelligence products obtained in order to influence the behavior of the audiences present in the COE/FOE;
- fire support – should be used to generate second-order effects, consisting in modeling the behavior of interest audiences in the desired direction;
- protection – although this is important for all the components of operational capability, its main effort should be to protect the morale of fighters, representing *"a product of the synergy of all the components of combat power"* (AC 71940, 2017, p. 3-8);
- sustainment – should be substantially amplified, assuming its fulfilment from a JIIM perspective;
- movement and maneuver – used on the principle of *maneuvrist approach*, it will allow significant amplification of combat power by developing constructive activities (involves the employment of the moral component of supporters and neutral parties), before launching the disruptive actions against the opponent (involves the employment of moral, conceptual and physical components); the principle of manoeuvrist approach is represented in *figure 2.*

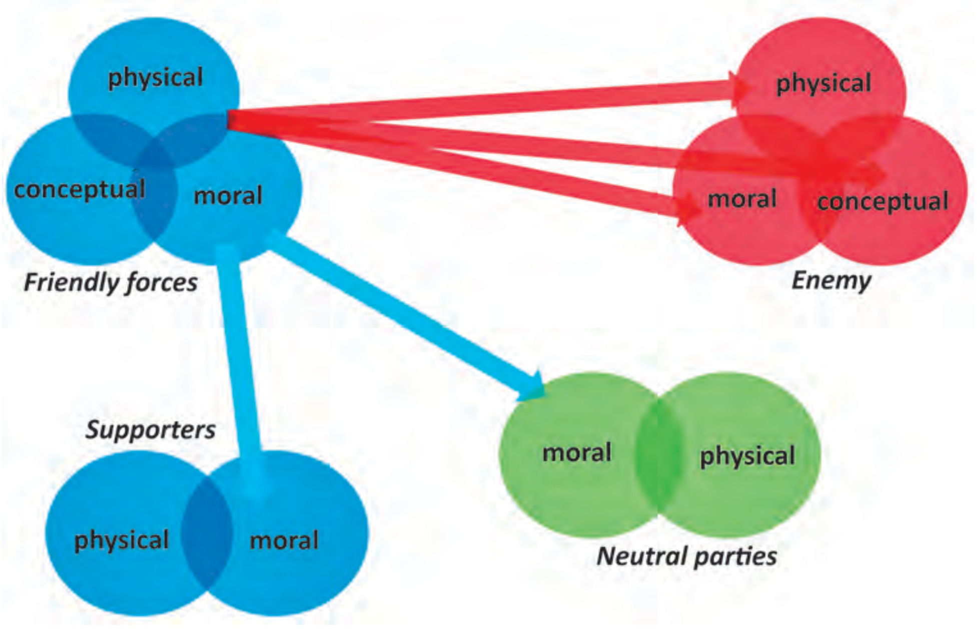


Figure 2: Increasing fighting/combat power – manoeuvre approach (Ducheine, Haaster, 2014, p. 7)

On these adjustment principles and adding engagement as a new WFF, the initial configuration of combat power (table 1) is transformed into the one in table 3.

Table 3: Combat power adapted to the COE/FOE requirements (Tudorache, 2020, p. 85) (a version)

	+ leadership (multiplies and unifies the combat power elements)			
Combat power	WFF	*intelligence* information activities are included	*engagement* allows relationship between military force and unified action partners (TRADOC Pam 525-8-5, 2014, p. 5)	*movement and manoeuvre* applied as manoeuvre approach
		fires aimed at modelling the behaviour of audiences	*C_2* applied as mission command	*protection* main effort on protecting the warriors' moral
			sustainment performed from JIIM perspective	
	+ information (understood as communication between structures)			

Further developing the issue of operational adaptation of military structures, the adjustment of combat power (table no. 3) generates implications at the level of planning methodologies, especially at the tactical level, involving adjustments to the military decision making process *(Military Decision Making Process – MDMP)*.

ORGANISATIONAL IMPLICATIONS

The operational adaptation of military structures to the requirements of operating within the COE/FOE automatically generates an adaptation of the organisational structure able to direct the adjusted combat power. This adaptation of the organizational structure should be done, both at the level of the HQ and for organic CBT, CS and CSS forces. A variant of tactical modular structure able to support the adapted combat power is presented in figure 3. This structure of the infantry battalion is designed for *Stability and Support Operations (SASO)*, given that the estimates of military specialists state that most likely such structures will be used for to perform SASO within the FOE.

Analysing the organisational structure above, at the level of the HQ the main adjustments consist in:

- development of cultural capability by integrating cultural experts *(Subject Matter Expert – SME)*, cultural advisers *(CULAD)* or foreign area officers *(FAO)* within the established modules (S_2, S_3, and so forth) or in the framework of another on its own; these new elements will facilitate the operationalisation of the cultural aspects specific to the other interest audiences in the operations process;

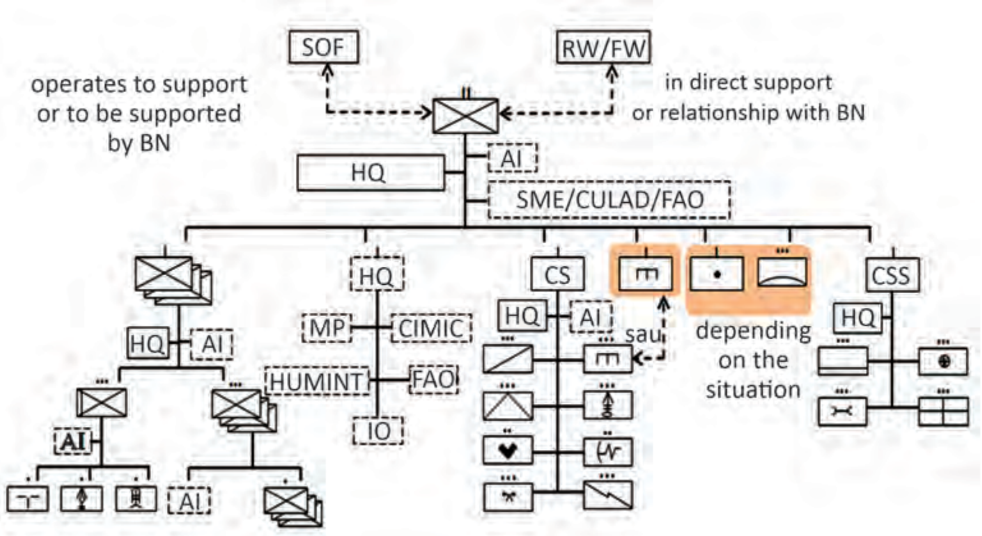

SOF
RW/FW
operates to support or to be supported by BN
in direct support or relationship with BN
HQ
AI
SME/CULAD/FAO
HQ
MP
CIMIC
HUMINT
FAO
IO
CS
HQ
AI
sau
depending on the situation
CSS
HQ
AI
AI
AI

Figure 3: Tactical modular structure for SASO (Ibid, p. 104)

- AI integration, at least within modules S_3 and S_2, for optimizing the information cycle, COP development and the support for its understanding, optimising the activity of the Tactical Operations Centre *(TOC)*, support for the adjustment decision-making during execution, and so one.

On the other hand, at the force level, some adjustments of their organization are given by:

- CBT – the company's command should be supported by AI capabilities for the purpose of advising it; infantry platoons and fire support platoon, by integrating AI into them, in the form of Lethal Autonomous Weapons *(LAWs)* will have improved capabilities on the efficiency and effectiveness of firing;
- CS – on the principle of CBT forces, the CS could also be augmented with AI capabilities in order to amplify firepower able to provide CBT forces with robust fire support;
- HQ – this company will support the battalion HQ in the exercise of engagement as WFF (table no. 3), having mandatory in its organic elements such as military police *(MP)*, specialized in civil-military cooperation *(CIMIC)*, dedicated to obtaining information from human sources *(Human Intelligence – HUMINT)*, FAO, other elements specialised in carrying out information operations *(IO).*

Therefore, the adapted combat power can be directed within the COE/FOE to the decisive place and moment, by adjusting the organisation of the HQ, on the one hand, and on the other hand reconfiguring the organisational structures of the subordinate forces, regardless of their typology.

CONCLUSIONS

At the end of this article, it can be concluded that the operational adaptation of forces should have a continuous character, because both the COE and especially the FOE have an accentuated dynamics, constantly changing their physiognomy. What is certain is that the operational adaptation aims as an end state to develop those capabilities that allow forces to operate in VUCA-type environments, regardless of their amplitude.

The operational adaptation should also be done taking into account the standards of military capability development with leadership implications by developing mental agility and building the expeditionary mentality. As expected, the greatest impact of the development of these standards occurs at the level of forces, involving the development of operational flexibility, promoting modularity and versatility, improving tactical mobility, and the AI integration.

The main challenge that arises is the difficulty of developing these capabilities on short term and in complete volume, and in this regard, we should prioritise or, in other words, we should find the answer to the following question: *What standard/standards should we start with to obtain operational adaptation?*

Given that the main effect of adaptation is change, we should start with operational flexibility, but not from an overall perspective that would involve meeting the other standards, but strictly focusing on the formation and development of a high capacity for immediate response.

Finally, in order to adapt the military structures to the requirements of operating within the COE/FOE, achieving the high immediate reaction capacity of the deployable force can take shape by reconfiguring the existing combat power, rethinking the established planning methodologies and, last but not least, reorganizing the CBT, CS, CSS forces.

BIBLIOGRAPHY:

1. Ducheine, P., Haaster, J. (2014). *Fighting Power, Targeting and Cyber Operations*. Amsterdam: Center for International Law.
2. Karaoguz, A.A. (2016). *Preparing to be Unprepared: Ground Force Commander Decision Making in a Volatile, Uncertain, Complex, and Ambigous World*. Monterey: Naval Postgraduate School.

3. Tudorache, P. (2020). *Adaptarea structurilor militare din Forțele Terestre la cerințele acțiunii în medii VUCA și JIIM*. Sibiu: Editura Academiei Forțelor Terestre *"Nicolae Bălcescu"*.
4. Wade, M.N. (2015). *BSS5 Smart Book: The Battle Staff – Leading, Planning & Conducting Military Operations*. Florida: The Lightning Press.
5. AC 71940. (2017). *Land Operations*. Warminster: Land Warfare Development Centre.
6. ADP 3-0. (2019). *Operations*. Washington, D.C.: Headquarters, Department of the Army.
7. ADRP 6-0. (2012). *Mission Command*. Washington, D.C.: Headquarters, Department of the Army.
8. AJP-3.2. (2016). *Allied Joint Doctrine for Land Operations*. Edition A. Version 1. NATO Standardization Office (NSO).
9. JP 3-0. (2017). *Joint Operations*. Joint Chiefs of Staff.
10. JP 2-01.3. (2014). *Joint Intelligence Preparation of the Operational Environment*. Joint Chiefs of Staff.
11. TRADOC Pam 525-8-5. (2014). *U.S. Army Functional Concept for Engagement*. Virginia: Training and Doctrine Command.

RELATIONAL APPROACHES TO THE RESILIENCE OF OPERATIONAL LOGISTICS

Colonel Prof. Gheorghe MINCULETE, PhD

"Carol I" National Defence University, Bucharest

The demands of modern warfare imposed by technological innovation and digitalisation have made operational forces prepare and act in a highly complex confrontational environment, which entails increasing resilience and flexibility.

The management and execution structures of the logistic support systemically integrated in the operational devices of the joint forces are prepared and act in their turn in the conditions of increased risks, which causes them to become increasingly resilient.

Knowing that during the two Gulf conflicts, the logistic losses of the responsible structures far exceeded those of the fighting and support forces, I consider that it is all the more necessary to study, design and implement the requirements to increase resilience of the operational logistical forces, for the fulfilment of future missions.

In this scientific communication I address, from a relational point of view, the issue of resilience of logistics systems (subsystems) integrated with operational forces acting at the tactical and joint levels.

Keywords: joint operations; operational forces; logistical support; resilience; operational logistics;

INTRODUCTION – GENERAL APPROACHES

The continuing military challenges of today's security environment are based on important technological innovations and multiple action determinants at strategic, combined and tactical levels. Under these conditions, modern operational forces must have capabilities, time and manoeuvrability, which can be provided and supported by dynamic, modular, flexible and efficient logistical support structures.

The increasingly asymmetric nature of current armed conflicts determines the design, preparation and conduct of joint military operations. Under these conditions, the logistical support of the action forces must allow simultaneous, successive and/or independent operations.

The operations specific to the war of the future are based on viable, dynamic and force multiplier logistics systems (subsystems), available to operational commanders, which allow obvious advantages (in terms of combat potential) in possible confrontations with the forces of any opponent. To this end, own operational logistics must support with materials (of all classes) combat platforms, high-precision weapon systems (of all types), armoured vehicles, vehicles, aircraft, warships etc. in view of the rapid deployment of forces and means (resources) necessary for their engagement in multinational operations, of joint type, conducted at national level under the auspices of NATO or directly by the commands of the Alliance (Sheikh, Mark & Dagher, 2016, p. 3).

The preparation and engagement of all the mentioned forces and means require the development, testing and implementation of specific strategic, joint and tactical plans, as well as the evaluation of results (based on performance indicators) in order to operate changes that will lead to continuous improvements in the future.

PARTICULARITIES OF THE RESILIENCE OF OPERATIONAL LOGISTICS

The concept of resilience is used in various forms by the US and NATO military structures in order to develop viable scenarios, build and train operational forces in peacetime. To this end, a combination of strategy and tactics is achieved with logistics by employing all types of resources, according to the requirements of military operations, taking into account all parameters of resilience in critical situations.

Military experts appreciate that from an operational point of view, the concept of resilience is: *"the ability of a force to resist the attack, to adapt and generate enough fighting power to achieve the objectives of the campaign ... despite the disruptions, regardless of whether they are natural or man-made ...". (Figure no. 1)* (Steeneck & Breitbach, 2019, p. 5).

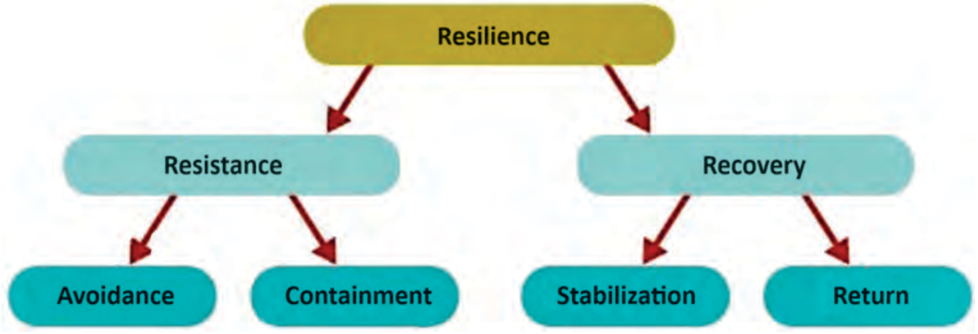


Figure no. 1: Components of the resilience of a military operational system (Ibid.)

From our point of view, *a military operational system, which also integrates a logistical support subsystem, is resilient when it resists any disturbances that would alter its normal functional performance. Figure no. 2* shows the operation of a system (subsystem), which can also be operational logistics, under conditions of resilience. This is determined by the destructive (disruptive) factor, following that in a given period of time the affected part of the system (subsystem) will be restored with its own recovery possibilities (capacities) (and with the support of the upper echelon – in case of operational logistics).

According to the assessment of US military experts, *resilience* is also analysed and measured in the field of military logistics based on several *performance indicators*. Following the analysis, we consider that *three performance indicators* can be used in the space of operational logistics (from the structure of a combat force), which can express the resilience of a logistics system (subsystem) at a given time (Steven et al., 2015, pp. 7-10).

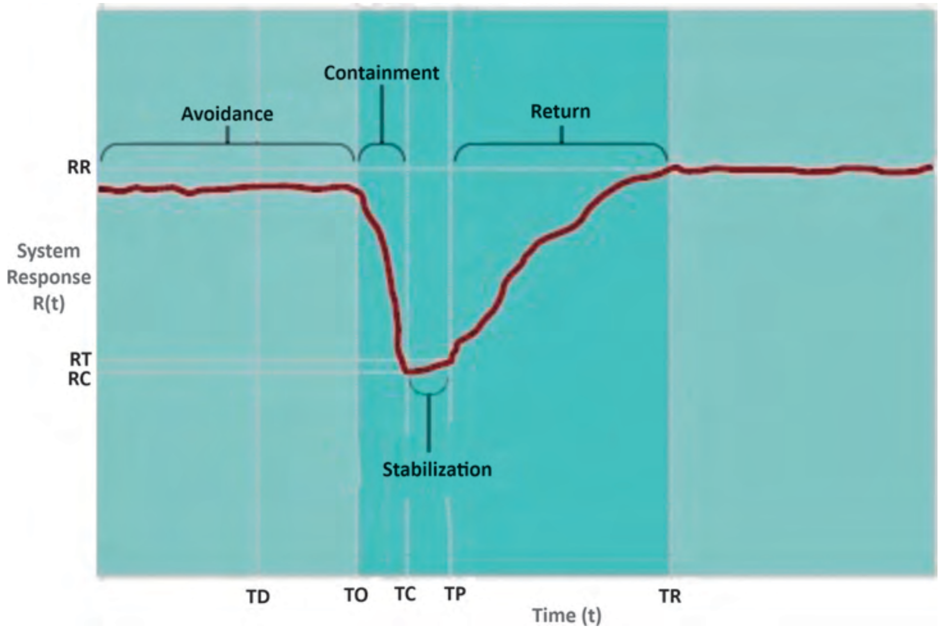


Figure no. 2: Resilience model possible in operational military logistics as well
(Steeneck et al., ibid., Steven et al., 2015, p. 247)

A first indicator would be, for example, ***the appropriate mission rate (Ram)***, which, in our view, is the ratio (percentage) of the total capabilities required by the mission (total operational support requirements in terms of logistical support areas) determined individually ***(Csfds)*** and total capabilities available for the mission (on the same areas of logistical support established and analysed individually – ***Cdmds),*** weighted at 100.

$$\text{Ram} = \frac{\text{Csfds}}{\text{Cdmds}} \text{ x } 100$$

Given the effect of the disruptive factor, in the process of assessing the resilience of operational logistics, from our point of view, another indicator can be used, namely the ***performance rate of the logistics system (subsystem) after its interruption (Rpsdi).***

This indicator is the result of the ratio between the remaining performance level (utility) of the force logistics system (subsystem) (***Nrps***) and the initial performance level (utility) of the same system (***Nips***), weighted at 100.

Basically, ***Rpsdi*** represents the ratio (percentage) between the level of total remaining performance (total capabilities remaining available for the mission on logistic support areas established and analysed individually, i.e. ***Nrpd***) and the initial level of performance of the logistics system (all initial requirements to support the operational force on areas of established logistical support – determined individually, i.e. ***Nipd***).

$$\text{Rpsdi} = \frac{\text{Nrpd}}{\text{Nipd}} \times 100$$

A third indicator, considered by us to be very important in assessing resilience, is ***the rate of recovery of the performance of the respective logistics system (subsystem) – Rrps*****.** One way of determining this indicator is, in our view, the result of the ratio between, the (total) level of operation of the logistics system (subsystem) mentioned – after the recovery of the damaged or destroyed part – ***Nfsr,*** at the level of initial (total) operation of the same system – ***Nfis*** (as total utility in support of the operational force), weighted at 100.

Therefore, ***Rrps*** is the percentage result of the ratio between the level of operation of the logistics system after recovery (total capabilities existing after recovery of those neutralised (by the opponent) to the related logistics support areas, established and analysed individually, i.e. ***Nfrd***) and the level (total) of the initial operation of the logistics system (includes all the requirements to support the operational force through the considered areas of logistical support – with individual determinations, (i.e., ***Nfid)***, weighted at 100.

$$\text{Rrps} = \frac{\text{Nfrd}}{\text{Nfid}} \times 100$$

Given the complexity of the data and information to be used in a short period of time, the three specified performance indicators are useful insofar as the digitisation of operational logistics in the military organisation, where the resilience assessment is performed, is appropriate.

MAIN FACTORS TO INCREASE THE RESILIENCE OF A LOGISTICS SYSTEM (SUBSYSTEM) IN THE OPERATIONAL FORCE STRUCTURE

In order to strengthen the resilience of a logistical system (subsystem) in the structure of an operational force of tactical or operational level, we consider several important factors, which will be presented below:

- ***Current, real and accurate information*** *is needed in the processes of planning/scheduling logistics operations*. Due to inaccurate information received from subordinated operational structures, timely and sufficient replenishments cannot be carried out, thus reducing logistical resilience. In this context, the actions of the fighting and support forces of the military organisation engaged in the operation will inevitably be affected (Snyder et al., p. 15).

Therefore, even small errors in the reporting of information and logistical data can sometimes have undesirable effects on the fulfilment of missions received by tactical military structures. However, errors sometimes occur either accidentally or due to cyber-attacks carried out by opposing forces. That is why, with certain structures and protection facilities received in support, the logistics forces of an operational military organisation should be strong enough to deal with errors and counter cyber or other attacks by opposing forces (Ibid., p. 16).

- ***Certain and flexible replenishment*** is *very important in the situation where significant quantities of material stocks have been destroyed by the opponent*, being necessary to replenish them by rapid replenishment from other existing military or civilian sources, identified by specialised bodies in the area of logistical responsibility of operational force or from sources distributed and made available by the upper echelon (Muller, 2011, p. 25).
- ***The capacity*** highlights the available backup sources, taking into account the costs of the technical and armament systems that need to be re-ensured to the troops. Therefore, for this purpose, it is very important to decide the locations where additional stocks will be set up, necessary both for increasing the operational potential of the theatre and for the continuous operation of the military supply-distribution chains. It would also reduce delivery and transport times in order to replenish the resources needed for combat and support forces in the structure of tactical and/or operational military organisations (Timothy et al., 2019, pp. 8-19).
- ***Visibility of interruptions***. The rapid recovery of military logistics systems (subsystems), affected and functionally disrupted by enemy strikes, is very important for the fulfilment of missions received by operational force structures. Thus, there is a need to ensure increased resilience for each area of logistical support (Muller, ibid., pp. 55-70).

In this regard, for the military logistics managers, the real operational images of the subordinate logistics systems (subsystems) are very important, so that they can make immediate decisions to sustain the fighting and support structures in order to directly counteract and surprise the opponent's actions.

• ***Adaptability***. A military logistics system (subsystem) can be adapted as a result of the modification or change of operations, in response to a certain type of disruption (Sarode et al., p. 59).

If we are considering replenishing materials from an available source (for example: military or civilian depot) that have been hit by the enemy, then it will be decided immediately to switch to supplying the same materials from one or more spare sources (military or civilian). At the same time, there will be an adaptation of the supply-distribution chains, according to the determined requirements of change, taking into account the urgencies of replenishments to the structures of the operational force, for certain classes and quantities of materials.

In the event that a company providing maintenance services was hit by the enemy, then the logistics manager of the respective operational structure will decide to use another existing (reserve) provider operator in the area of logistics responsibility. This will also determine an adaptation of the evacuation-r e pair-return chain of the technical systems from/to the fighting and/or support subunits.

•***Anticipation***. In order to ensure a high resilience of a logistics system (subsystem) (belonging to an operational military organisation) the actions of logistics managers are very important, adequate to predict and/or analyse possible threats, attacks or disruptions, produced by enemy forces (terrorist groups, reconnaissance, deception or special forces) (Ibid., p. 72).

This situational awareness of the need for protection, effectiveness and efficiency of logistics forces, in the dynamics of military actions, requires a continuous collaboration of the logistics module with the modules of information (intelligence) and operations of the staff of the operational force, while conducting a risk management normalisation of all areas of logistical support. In this regard, there will be a continuous monitoring of the functioning of the support (logistics) structures during the continuous development of the flows of products, assets, materials and services to/from the troops (Ashurst&Beaumont, 2020, p. 3).

•***The recovery or restoration of the operation to the initial parameters*** of a logistics system (subsystem) represents its capacity to return to the normal state, by the gradual attenuation of the functional interruption. As a rule, based on effective actions specific to risk management, the possibility of accelerating the recovery or restoration of the normal functioning of the respective logistics system (subsystem) is foreseen before the damage caused by the interruption of support (logistics) to units or large operational units increase in intensity or even multiply (Jansen et al., 2014, p. 27).

In the above-mentioned context, if at any time there are a large number of armoured vehicles and transport vehicles that require immediate repairs in order to restore their functionality, then the competent logistics authorities will request early/immediate support from the upper echelon and local public administration, to provide the operational structures with the necessary repair capacities, as well as the technical means of combat necessary to replace the unavailable ones (in case of impossibility to repair them).

In this way, the risks of not fulfilling the missions received by the large units and/or tactical units will be diminished as much as possible, as a result of the forced change (interruption) of the courses of their offensive or defensive actions. Actions to restore functional capacities may also take place in the operational force's warehouses or in other formations in the composition of its action structures. Here, both the reconstitution of material stocks and the replacement and/or repair of transport vehicles destroyed by the attacks of the opponent forces are considered. It follows, therefore, that until the recovery (restoration and reconstitution) of the neutralised capabilities, the upper echelon will provide the operational force with adequate logistical support structures (material echelons, logistical support echelons, maintenance and evacuation modules, medical support modules etc.)

• ***Dispersion***. In order to reduce the interruptions of the normal operation of a logistics system (subsystem), logistics module managers must collaborate with operations and information structures in order to have dispersed in the field of logistics support functional execution structures (transport units and subunits; warehouses; maintenance structures; medical structures; self-support and protection structures etc.), so that their losses because of air, ground, naval strikes, including drones, can be as low as possible. At the same time, the centralised arrangement of the logistics systems (subsystems), in certain situations, in order to obtain effectiveness and efficiency, is in dissonance with the dispersion, according to the specific implementation requirements.

Given the analyses of military experts, it is necessary, since peacetime, to achieve as realistically as possible the interoperability objectives of both operational forces and logistical support structures in their staff (Ashurst& Beaumont, p. 4). In this way there is the possibility that, in time, adequate resilience of logistical support will be achieved during the conduct of operations, anticipating the gradual decrease of resources to be provided to combat forces over a period of thirty days, due to increased consumption and the actions of the adversary. *(Figure no. 3)*.

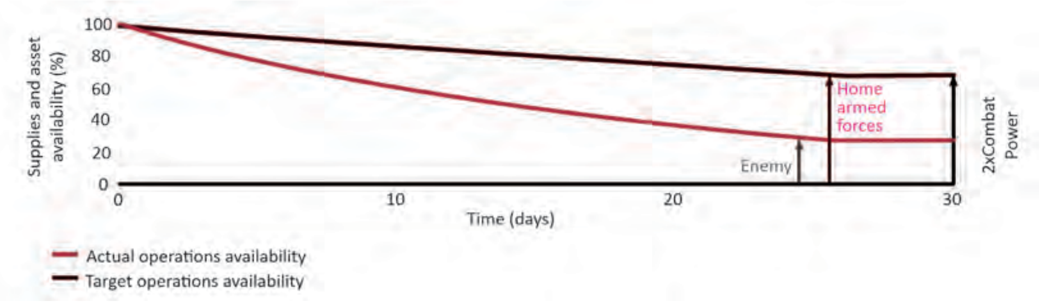


Figure no. 3: A graph of the decrease in logistical resources required for support operational forces (Sheikh et al., 2016, p. 5)

For an operational force, the logistics unit (subunit) in its structure must be efficient to support sufficiently and timely combat forces before a crisis caused by the opponent's blows, while having the availability of rapid recovery, so that it can adequately support the fighting and support structures.

For this purpose, in order to fulfil the mission of the operational forces, a particularly important role is played by capitalising on the potential of interoperable and integrated logistics systems and capabilities in their structure, so that if they act in a theatre (area) of joint operations within the Alliance to be able to achieve the necessary logistics support in order to reach the objectives in the dynamics of their planned military actions (Ashurst&Beaumont, p. 5).

Given the instrumentation of the requirements of logistics 4.0, the resilience of operational logistics can increase through agility and support capacity, thanks to the new facilities offered by digitisation. Therefore, the development of real-time support activities of combatant military organisations through the resources involved in logistics 4.0 (implemented in the military field), generates a number of specific risks, which requires adequate security and cyber protection, but also functional systems (logistics profile, digitally and physically connected) of much better performance (Rahim et al., 2018, pp. 15-25).

From our point of view, the proactive and anticipatory conduct of logistics managers will determine them to take into account the forecasts resulting from the analysis of the factors of increasing the resilience of a logistics system (subsystem) (from the operational force structure, mentioned above), so as to develop and apply risk management guidelines specific to the areas of logistical support. Therefore, these procedures will allow, during the development of the operations, to be avoided as much as possible: stockouts at the operational structures; failure to ensure in a timely manner the combat systems necessary to replace the destroyed ones; the impossibility of performing the evacuations of the wounded and of combat assets; the impossibility to carry out the repair operations of the equipment evacuated from the staff of the combatant subunits (units, large units); insufficiency or crisis of adequate means and materials for medical support etc.

CONCLUSIONS

The current changes in the theory and practice of modern warfare determine that both the operational forces and the related logistics operate modularly, flexibly, dynamically and in conditions of high resilience.

The peculiarity of the resilience of a logistics system (subsystem) in the staff of an operational force reveals the phases of resistance and recovery (partial or in full) through appropriate and measurable variables.

The construction of a resilient logistics system (subsystem) for an operational force must ensure that the management capabilities of the leading logistics subsystem are balanced with the capabilities and vulnerabilities inherent in the managed logistics subsystem (including logistics support execution structures) in order to respond immediately to enemy attacks, for the rapid recovery of the affected party/parties and then (after a relative interruption) the appropriate logistical support actions of the operational force components.

However, under proper logistics management, a high level of resilience of the managed logistics support system can be achieved by ensuring the necessary balance between its available capabilities and the inherent vulnerabilities.

In the same framework of analysis, it is necessary to take into account past disruptions (with the necessary corrections) in correlation with the experience and availability of anticipation, recovery and adaptation of logistics systems (subsystems) of operational military organisations to requirements, in order to fulfil missions that come back to them in crisis situations and in war.

At the same time, we are of the opinion that the tactical and joint operations of the future, within the groups of forces led by national and/or NATO structures, require that both commanders, management and execution structures of logistical support, and other officers they collaborate with to know and apply, in the new conditions imposed by automation, robotisation and digitisation, all the methods, techniques and procedures necessary to increase the resilience of operational logistics in order to successfully overcome situations of risk and uncertainty, to ensure continuous development and to obtain success in offensive, defensive or other operations against any opponent (aggressor).

BIBLIOGRAPHY:

1. Ashurst, T., Beaumont, D. (2020). *Logistics interoperability a valued asset, strategic enabler in the US Army*. In Army Sustainment, https://www.army.mil/article/231663/logistics_interoperability_a_ valued_asset_strategic_enabler, retrieved on 12 September 2020.
2. Jansen, M., Trépant, H., Lamaa, A., Andrew, S. (2014). *Achieving information superiority: Five imperatives for military transformation*.
3. Rahim, A., Rahman, A., Rashid A.S., Raihan, N., Hamid, A. (2018). *Agility and digitalization competency in logistics 4.0 in military setting: the challenge, risks and opportunities*. In Asian Journal of Social Science Research. Vol. 1, no. 2, https://www.researchgate. net/publication/331634349, retrieved on 3 August 2020.
4. Snyder, D., Bodine, B.E., Amouzegar M. A., Lynch, F.K., Lee, M., Drew, G. J. (2017). *Robust and Resilient Logistics Operations in a Degraded Information Environment. RAND Corporation*. California: Santa Monica, https://pdfs.semanticscholar.org/c938/19f65fd04499d8fcfeccf5e61e0c 74474f14.pdf, retrieved on 3 August 2020.
5. Sarode, A.D., Lokmanya, T., Khodke, P.M. (2009). *Performance measurement of supply chain management: A decision framework for evaluating and selecting supplier performance in a supply chain*. The International Journal of Applied Management and Technology. Vol. 1, no. 1, https://www.researchgate.net/publication/241838507, retrieved on 12 September 2020.
6. Sheikh, H., Mark, B., Dagher, S. (2016). *Resilient and agile making logistics a combat multiplier for GCC armed forces*. In Strategy&formerlyBooz&Company, Linkedin, https://www.strategyand.pwc.com/m1/en/reports/resilient-and-agile.pdf, retrieved on 3 August 2020.
7. Steeneck, W.D., Breitbach, T. (2019). *Exceptional Release Presents. Resilient Sustainment*. In Logistics Officer Association, https://atloa.org/er-resilient-sustainment/, retrieved on 12 September 2020.
8. Steven, A.M., David, J.C., Stanley, E.G., Christopher, W.Z., John, R. (2015). Macdonald, *Understanding Supply Chain Resilience*. In Supply Chain, http://www.supplychain247.com/article/understanding_supply_chain_resilience/, retrieved on 12 September 2020.

9. Timothy J., Pettit Keely, L., Croxton, J.F. (2019). *The Evolution of Resilience in Supply Chain Management: A Retrospective on Ensuring Supply Chain Resilience*. In Journal of Business Logistics. Vol. 40, no. 1, https://onlinelibrary.wiley.com/doi/10.11 11/jbl.12202, retrieved on 12 September 2020.

WAYS OF EMPLOYING ISR STRUCTURES FROM LAND FORCES IN EXERCISES CONDUCTED ON NATIONAL TERRITORY

Lieutenant-Colonel Valeriu-Adrian JIANU

PhD student, "Carol I" National Defence University, Bucharest

The ISR structures (Intelligence, Surveillance, Reconnaissance) of the Land Forces participate constantly in exercises on national territory, bringing a substantial contribution to intelligence support of decision-makers in all operation stages.

Through their specific capabilities, ISR structures will cooperate uninterruptedly both horizontally and vertically in information gathering. Digitalising, applying information technology on ISR capabilities will provide the commander and his staff with multiple levers that will enable him to make decisions much quicker and to exploit the resulting plan much more efficiently, thus reducing the duration of operations.

Keywords: information; research; surveillance; Land Forces; crisis situations;

INTRODUCTION

The world is constantly changing, on the one side, as a result of the continuous development of technology, and on the other, due to the impressive findings resulting from ample research being done, as well as from the desire to optimise the processes of gathering information in all fields of combat.

Starting from the nation's security objectives referring to *"developing the national capacity of a state to defend itself"* and *"increasing the efficiency of national systems for prevention and management of crisis situations"* (*Strategia Națională de Apărare a Țării/The National Defence Strategy*, 2020, p. 14), we consider it necessary to address the possibilities of supporting ISR structures in Land Forces in the combined effort of the information architecture gathered during national exercises. Thus, at national level, the combined intelligence, surveillance and research system is essential for all military operations, as it provides intelligence to decision-makers and staff, thus creating the necessary conditions, on the one hand, for the adoption of correct and timely decisions, and on the other hand, for the successful accomplishment of military actions and operations.

THE OPERATIONAL ENVIRONMENT OF THE FUTURE

From a doctrinal point of view, the concept of ISR is *"a set of intelligence and operations capabilities that synchronise and integrate the planning and operations of all collection capabilities with the processing, exploitation and dissemination of resulting intelligence, in direct support of planning, preparation and execution of operations"* (*Doctrina pentru proceduri de informații/Doctrine for Intelligence Procedures*, 2018, p. 10).

At the same time, the Joint Intelligence Surveillance and Reconnaissance (JISR) initiative was launched by NATO at the 2012 Chicago Summit as a complex, extensive and significant area of capabilities. The allies also intend to work together to promote the exchange of information, using NATO platforms and networks and optimising their use to develop the joint effort in the field of JISR (Warsaw Summit Communiqué, Art. 75).

JISR is a multidisciplinary approach, containing four distinct elements: joint, intelligence, research and surveillance. The joint concept represents the integration of activities, operations and organisations in which at least two participating elements take part (AJP-3.3, p. 15).

During the joint exercises carried out on national territory, based on the documents received at the strategic level, the commander of the Joint Forces Group identifies the intelligence and training requirements specific to the ISR structures of the Land Forces. These structures participate in the full spectrum of ISR operations that are defined in the literature as *"operations performed by forces that have the main mission of collecting data and information, as well as other forces that have the ability to perform such a mission as a secondary mission"* (IA-1.5, p. 9).

ISR operations aim to gather intelligence on the enemy, terrain, weather and other relevant aspects of the area of operations, aspects that can influence the actions of their own forces. Approaching the perspective of carrying out actions at operational level in the national ISR spectrum, we are aware that they take place in a fluid, multidimensional environment, characterised by asymmetric types of actions, mobility, decentralisation, manoeuvrability, flexibility and using a very wide range of combined actions such as air, land, naval, information, psychological carried out simultaneously, at a very sustained pace.

During the exercises, ISR structures of the Land Forces will train in carrying out missions specific to the ISR domain, which represent, from a doctrinal point of view: *finding clues and early warnings, preparing joint intelligence on the operational field, identifying the combat organisation and disposition of enemy combat forces, estimating and monitoring the situation, support for force protection and help for the process of target management* (I.A-1.5, p. 10).

The future operation environment will be characterised by *"constant and essential changes"* (Air Force Doctrine Document, 2007, p. 15). The digitalisation of the modern battlefield, the dominance in information and psychological confrontations, the shaping and simulation of battle actions, the modularity are all aspects that, through a permanent improvement, have considerably changed the physiognomy of combat. Therefore, it can be stated that the war of the future will take place mainly in the information field: *"Know your enemy and know yourself; out of a hundred battles, you will not expose yourself to any danger!"* (Sun Tzu, 2009, p. 24). Current trends reveal that new types of wars are gradually required, such as: information warfare, cyber warfare, network-based warfare, electronic warfare, psychological warfare, media warfare etc. (Paul, 2005, p. 13).

In the present approach, respectively that of the possibilities of using ISR structures in exercises on the national territory, we consider that we have to take into account several aspects. Throughout the national territory, we have a multitude of specific capabilities. All these, used in an optimised framework, can generate multiple ways of developing high-performance skills in carrying out actions at an operational, combined level. Therefore, the ISR structures of the Land Forces apply their principles, which, regardless of the echelon, consist of: *centralised targeting and decentralised execution, responsiveness, sharing, sustainability, trust and accuracy* (I.A-1.5, 2017, p. 17).

In order to highlight possible exercises, we need to consider all the environments in which state actors can participate, especially the capabilities of all services. Referring to Joint – type exercises, in which there will be a cooperation between the ISR availabilities of all spectra, the type of JISR system is the integrator of terrestrial, aerial and naval images (Land Recognised Picture-LRP, Aerial Recognised Picture-ARP, Naval Recognised Picture-NRP) and, at the same time, the element that meets the information requirements necessary for the conduct of military actions.

Specific to their activity is the creation and dissemination of images through specific systems, such as: Land Forces IRS Capabilities Integrated Command and Control System/SIC2SR; National Air Command and Control System/SCCAN; Integrated System for Observation, Surveillance and Control of the Traffic at the Black Sea/SCOMAR. To achieve joint interoperability, ISR systems will be structured on three components:

- a command and control component;
- a data and information merging component;
- a data and information collection component (Delivering Actionable Intelligence, 2011).

The operational ISR support network is, in fact, a *"system of systems"*, multiple networks interconnected at different levels of classification, connecting different structures. In this context, the information must be accessible to all beneficiaries, regardless of their position and field of activity, through network access and security policies, so that both their levels of access to classified information and the principle of *"the need to know"* are respected. By networking all available sensors and sources, the capabilities can now merge data with other sources, add details to the COP (Common Operational Picture) and support a wide range of beneficiaries.

In contemporary and future military actions, land forces groups will be reduced in number, but at the same time will benefit from the support of high-tech combat and ISR structures. All operational structures will be of the combined weapons type, with a special independence of action, and will be set up on the principle of combat groups, for complex actions in any range of terrain, regardless of its degree of accessibility (Udeanu, 2006, p. 64). This aspect of military action highlights the fact that, *"regardless of the level of modernisation of air or naval military structures, in the contemporary stage and in the immediate perspective, the conquest and control* *of ground space remain a priority and final objective of any strategic operation”* (Ibid, p. 63).

According to some specialists in the field, the battlespace represents *“the environment, factors and conditions that must be understood for successfully applying the combat power, providing force protection and fulfilling the mission. It includes air, land, sea, space and the elements existing in them: own and enemy forces; disposition; weather conditions; land; electromagnetic spectrum; the information space in the area and the area of interest”* (Mathews, 1997, p. 71).

If we analyse the way in which ISR structures p erform in exercises, from the perspective of work environment, we can apply a high rate of presence in all spaces where battle can take place: land, air, extra - atmospheric, cosmic and geophysical spaces.

At the same time, in most of these cases, *“the area meant for military actions is not identified only with the land, air and maritime space necessary for this purpose, but rather with the conditions of time, season and weather”* (Pantazi, 2007, p. 79).

In addition, we are witnessing the emergence of new combat spaces, generated by the military technological revolution, specific to modern warfare, that are improper to physical (natural) space. We can recognise, in this case, the following types of spaces, with their own dimensions and characteristics, in which the ISR structures also carry out their specific activities: the information space; computer space; virtual space (cyberspace); electromagnetic space; CBRN – meteorological – ecological space; psychological space; parapsychological space.

The optimisation of processes designed to create performance for operational cooperation between services can be achieved by involving and integrating, in various exercises, all ISR capabilities available at the national level, exercises which, through customised scenarios, train aspects related to the command-control, data and information fusion subsystem, obtaining results that will meet the following hypothetical requirements:

- it will ensure the command and control of the execution subsystem;
- it will direct and integrate ISR and target location system, in support of the level of operations command;
- it will plan and manage the collection process carried out by the execution subsystem in order to collect data, information, images from the area of intelligence responsibility or informational interest, depending on the scope of the exercise;
- it will integrate the execution subsystem into the ISR system, facilitating its coordination with other means of information collection;

- it will process, filter, integrate and exploit images, data, information and products resulting from their processing, from multiple sources, in order to meet information needs (including optical, infrared, multi-/hyperspectral images, images captured by the radar system with synthetic aperture, images recorded by terrestrial target motion sensors, as well as data and information provided by IMINT, SIGINT, HUMINT, OSINT sources or by independent sensors, CIMIC reports and other national sources);
- it will transmit raw/processed information to users (including for upper and subordinate command levels, air and naval forces), on time, in a secure and efficient manner, not only in visibility parameters, but also beyond them;
- it will put together and display the current situation of the information on the battlefield, with permanent and timely updates.

In addition, in any type of exercise, aspects of the execution subsystems related to the operation of each capability may be involved, in such a way as:

- to integrate capabilities into a wider system (JISR), taking into account the broad range generated by the media approach with the help of all services;
- to easily locate and identify targets in daytime, at night and in favourable or unfavourable weather conditions and to send the information in a timely manner to all branches (thus ensuring the coherent establishment of easy and efficient communication links);
- to use appropriate terminological skills to process and exploit intercepted communications;
- to cooperate with other means of collecting information (including components of the Romanian Intelligence Community, namely the Romanian Intelligence Service, the Foreign Intelligence Service, the General Directorate of Defence Intelligence and the General Directorate of Intelligence and Internal Protection of the Ministry of Administration and Interior);
- to disseminate information to beneficiaries in a timely and secure manner;
- to exploit shaping and simulation capabilities and their related systems in order to familiarise all participants with the modus operandi and the process of collecting, processing and providing data and information.

In our opinion, the participation of ISR structures in national exercises must necessarily include specific training regarding survival, avoidance of capture, resistance in conditions of isolation, capture or detention and escape-extraction-recovery. Survival, Evasion, Resistance and Extraction/SERE is *“a set of tactics, techniques and procedures designed to provide isolated personnel with the skills necessary for survival in a hostile environment and resistance in captivity”*

(SMAp.-61, 2020, p. 10). When captured by the enemy, the isolated personnel (ISOP) must face the physical and mental pressure exerted on them, and when the situation calls for it, to escape, either through support received from the recovery forces or by their own forces, by identifying ways back.

During the joint exercises, the ISR bodies must be ready for the risk of isolation. The risk o isolation can be added to the following categories: low risk of isolation or exploitation; medium risk of isolation or exploitation; or high risk of isolation or exploitation (Ibid, p. 19).

The ISR bodies prepare their teams for any mode of acting in case of isolation in a hostile environment. At the same time, the participating military personnel will be trained to limit the risk of exposure to isolation, through current plans as well as through specific operating procedures.

We also consider it necessary to intensify training, at joint level, of the ISR bodies of Land Forces for the collection of data and information from open sources (OSINT), which are explicitly focused on the intentions of opponents and operations carried out by potential opponents or even partners. Through open sources, ISR structures can support missions at operational level, such as: contributing to the identification of clues and issuing early warning; contribution with information to the targeting process: identification, location, prioritisation, loss assessment; evaluating efficiency from an operational point of view (I.A.-1.7, p. 16).

In order to participate in joint exercises, ISR structures are preparing information documents through a very good knowledge of the operational environment. The training, from the perspective of providing information from open sources, may include training and development of skills in: searching, identifying and accessing information in an optimal time; identifying the information needed to support operations and skills in identifying and processing relevant, timely and credible information; evaluating the information objectively; understanding the nuances of legality in the use of information from open sources (Ibid, p. 20).

Cyber Intelligence (CYBERINT) structures obtain information by intercepting data transmitted in the cyber environment, other than those obtained from open sources. CYBERINT operations are represented by *"intrusive or non-intrusive activities carried out in order to collect data and information necessary for the operational preparation of cyberspace"* (S.M.Ap.-74, p. 23). Intrusive activities are those carried out by exploiting enemy and private networks, while non-intrusive actions are the result of exploiting information from public and own networks.

Therefore, we can reckon that the ISR structures of the Land Forces, through the CYBERINT structures, can participate in the intelligence preparation of the operational environment of the cyberspace by developing intelligence products to support the process of planning and conducting operations and decision-making by the commander. The main lines of effort in the field of CYBERINT focus on: convergence towards common, clear and concise objectives and goals; streamlining the allocation of available resources; concentration of joint effort through cooperation and coordination (Ibid, p. 25).

Contemporary conflicts have shown that no land or naval operation can be carried out without air support. High impact strength, accuracy of air strikes and missiles, speed of reaction (moving by air is the fastest, of all other means of movement) gives this service a special importance in the planning, organisation and conduct of any military operation.

Space actions exceed the limit of human conditionality, taking place in outer space, in the immediate vicinity of the Earth's atmosphere, through the presence and action of artificial satellites, the main responsible for collecting information about space combat, in general, transmitting data and information in real time, as well as directing certain high-precision shots. The space environment does not involve a direct confrontation between conflicting parties, but it supports their actions and, in most cases, they become decisive in winning the war: *"Action in outer space is not the same as the battle to conquer the Cosmos. This type of conflict implies an unlimited, vertical expansion in the outer space of the theatres and the means of confrontation at the information, media, economic and military level"* (Mureșan et al, 2006, p. 56). ISR systems, location systems and other means can be placed in the space, thus facilitating the unlimited use of this environment in military confrontations.

The entire process of air operation planning and air defence is supported by the ISR process, enabling the continuous development of current and future operations. This process is closely aligned with the information requirements and needs to be coordinated to achieve mutual support between commands and to maximise the efficiency of collection and exploitation capabilities.

The ISR structures from Land Forces support the development of the JIPOE process (joint intelligence preparation of the operational environment) through information on: identifying the threats posed by risk factors, as well as assessing their evolutionary trends; the opponent's organisation: composition, identity, disposition, military equipment, possibilities of action, logistical support, particularities; possible enemy directions of action; possible intensity of military operations; possible time of air action; districts, targets and alignments that can be hit by enemy air means (FA-1.2, p. 32).

By supporting the joint intelligence preparation of the operational environment, ISR structures in the Land Forces can contribute intelligence related to the air threat, but also to the enemy air infrastructure, as follows:

- identification of airbases as well as temporary aerodromes;
- location of missile systems and infrastructure elements: supply, transport, storage, launch;
- identification of organisation of integrated air defence system (IAMDS Integrated Air and Missile Defence);
- environment and climate in the combined area of operations, as well as their effects on both own and adverse forces;
- identification of electronic warfare capabilities, location and how to use them;
- assessment of the strengths and weaknesses of the enemy, its vulnerabilities in different phases of the operation;
- observation, identification and analysis of the enemy measures of deception, masking and camouflage (Ibid, p. 34).

Naval military actions take place in rivers, seas and oceans both at the surface and in immersion. Due to the economic interests of the great powers in the maritime space, a source of raw materials, especially energy resources, the importance of confrontations on the seas and oceans of the world has increased dramatically. Thus, naval power has become an element of discouragement, intimidation or threat of the first rank, *“decisive in the design of the geopolitics of states and in their geostrategy”* (Udeanu, p. 67).

ISR structures in the Land Forces support naval structures through surveillance missions by surveillance of the maritime space. The viability of surveillance by observation is determined by the existence of networks of observation posts, links to high-performance communications, specific observation equipment, training of personnel regarding the maritime adversary. At the same time, the structures carry out the observation constantly and continuously, through a judicious organisation and distribution of forces and means, in a unitary conception, ensuring the transmission of data and information in a timely and efficient manner.

Maritime surveillance ensures: observation of own and enemy ships; identification of the characteristics of the main naval and air platforms; identification, warning and reporting of imminent attacks; reporting of data on weather changes.

Modern wars have demonstrated the interdependence between the services during the fulfilment of assigned missions and the need for a three-dimensional planning of actions. With the advent of the concept of *deep shot*, military theory and tactics have undergone a new evolution, imposed by the high technology of the military environment, the emergence of weapons and high-precision shots, which have demonstrated the need to improve planning and organisation of joint operations.

CONCLUSIONS

The impact of the unprecedented evolution of technology has generated a revolution on the battlefield, whether we are talking about real situations or referring to training environments, continuing to exert a considerable influence on the conduct of military operations, exercises and other training taking place in the national environment.

Digitisation, application of information technology on ISR capabilities will provide a commander and his staff with multiple levers that will enable him to make decisions much faster than before and exploit the resulting plan more efficiently, with the effect of increasing the rhythm of operations.

The exercises planned and carried out together, using all available capabilities, will provide coherence, generate skills and align the services with the use of all tools in order to obtain complex details about the operational environment.

Through the common exercises on national territory, the sensors of the Land Forces must be constantly connected to the sensors of Air and Naval forces, through a common network of information and communication, in order to create a fusion of information and avoiding duplication, congestions and redundancy, while at the same time respecting the principle of *“operating on the same map”* (IGEO-1 2020, p. 8), so as to provide a complete and objective image of the operational environment for the Joint Task Force.

BIBLIOGRAPHY:

1. Bălăceanu, I. (2001). *Revoluția tehnologică contemporană și impactul ei asupra potențialului militar.* București: Editura Academiei de Înalte Studii Militare (A.Î.S.M.).
2. Dumitru, D. (2007). *Mediul internaţional de securitate şi influenţa acestuia asupra artei militare*. Bucureşti: Centrul Tehnic-Editorial al Armatei.
3. Metz S.; Johnson, V. (2001). *Asymmetry and US Military Strategy. Definition Background and Strategic Concepts*. Washington D.C.: Strategic Studies Institute, Special Report.
4. Neagoe, V. (2005). *Elemente de teorie şi construcţie militară*. Bucureşti: Editura Militară.
5. Pantazi, S. (2007). *Tehnologia și acțiunile militare în era informațională*. Bucureşti: Editura UNAp *“Carol I”.*

6. Paul, V. (2005). *Conflictele secolului XXI. Războiul informațional*. București: Colocviu Strategic nr. 7, UNAp "Carol I".
7. Roceanu I. (2003). *Informaţia în sistemele C4I*. Bucureşti: Editura A.Î.S.M.
8. Mureşan, M.; Stăncilă, L.; Enache, D. (2006). *Tendinţe în evoluţia teoriei şi practicii războiului*. Bucureşti: Editura UNAp *"Carol I"*.
9. Stanciu, C. (2015). *Implicaţiile sistemelor şi tehnologiilor moderne în redefinirea unor noi concepte doctrinare*. Bucureşti: Buletinul U.N.Ap., vol. 2, no. 1.
10. Sun Tzu (2009). *Arta războiului*. București: Editura Litera.
11. Udeanu, Gh. (2006). *Elemente de strategie militară contemporană*. Bucureşti: Editura UNAp *"Carol I"*.
12. AAP-6, *NATO Glossary of Terms and Definitions*.
13. AAP 1001.3 (2011). *The Air Force Approach to ISR. Royal Australian Air Force*.
14. Air Force Doctrine Document 2-0 (2012). US Air Force: Global Integrated Intelligence, Surveillance and Reconnaissance Operations.
15. AJP-2.7 (2009). *Allied Joint Doctrine for Reconnaissance and Surveillance*.
16. AJP-3.2 (2016). *Allied Joint Doctrine for Land Operations*.
17. AJP-3.3 (2016). *Allied Joint Doctrine for Air and Space Operations*.
18. F.A.1.2. (2020). *Doctrina privind apărarea aeriană și antirachetă cu baza la sol.* București.
19. F.A.1.3.2. (2011). *Manual privind organizarea și executarea supravegherii prin observare a spațiului aerian și terestru/maritime*. București: Statul Major al Forțelor Aeriene.
20. *Foreign Affairs* (January-February 1997). Washington, D.C.
21. I.A-1.1 (2017). *Doctrina Informațiilor pentru Apărare*. București.
22. I.A-1.5 (2017). *Doctrina întrunită pentru informații, supraveghere și cercetare*. București.
23. I.A-1.6 (2018). *Doctrina pentru proceduri de informații*. București.
24. I.A-1.7 (2020). *Doctrina pentru informații din surse deschise*. București.
25. IGEO-1 (2020). *Instrucțiuni privind sprijinul geospațial în Armata României*. București.
26. S.M.Ap.-61 (2020). *Doctrina pentru recuperarea personalului în mediu ostil.* București.
27. S.M.Ap.-74 (2020). *Doctrina operațiilor în spațiul cibernetic*. București.
28. S.M.F.T.-20 (2019). *Manualul pentru întrebuințarea elementelor ISR din Forțele Terestre*. București.
29. *Strategia Națională de Apărare a Țării 2010-2024* (2020). Bucureşti. Administrația Prezidențială.
30. *Warsaw Summit Communiqué, issued by the heads of state and government, participating in the meeting, of North Atlantic Council in Warsaw*, 8-9 July 2016.

WEB SOURCES:

1. http://www.scritub.com/administratie/COMUNITATEA-DE-INFORMATII54521.php., retrieved on 13 September 2020.
2. https://www.raytheonintelligenceandspace.com/news/feature/complete-picture (Delivering Actionable Intelligence, 2011), retrieved on 3 October 2020.

3. https://balkanservicegroup.files.wordpress.com/2017/12/doctrine.pdf, retrieved on 15 September 2020.
4. https://www.dni.gov/index.php/what-we-do/what-is-intelligence, retrieved on 15 September 2020.
5. https://www.raytheonintelligenceandspace.com/news/feature/complete-picturewww.globalsecurity.org (Intelligence, Surveillance and Reconnaissance Operations, Air Force Doctrine Document 2-9 17 July 2007), retrieved on 3 October 2020.

THE DISPUTE REVIVAL FOR THE SUPERPOWER STATUS

Colonel (r.) Romică CERNAT, PhD

The resurgence of Russia and the rapid development of China have created a new period of rivalry for superpower status. The debates of the main global actors on the relaunch of competition have led to a review of the importance of the great strategy and geopolitics as a starting point for analysing the defence funding level, strategy, plans, and programmes.

The post-Cold War period of international relations, which began in the early 1990s and generally was referred to as the unipolar stage, with the United States as the sole superpower, passed into a new phase, marked by events with global consequences from 2006 until 2014. The international environment has shifted to a fundamentally different situation characterised by a resurgence of dispute by China and Russia and the challenges of these two countries to the specific mechanisms of the US-led international order, which operated even after the end of the First World War.

Counter-terrorism and other military operations in the Middle East, which have been the focus of discussions on military-specific issues following the 9/11 terrorist attacks, continue, but now are a less dominant element in US military concerns, other areas related to China and Russia becoming now relevant.

Keywords: competition; bipolar world; world superpower; international order; state actor;

INTRODUCTION

Strategic trends in recent years illustrate the accumulation of a substantial potential to reshape relations between actors with global interests, with direct effects on the stability and predictability of the international system, and the revival of global strategic competition confirms the transition to a new security paradigm (*The country's National Defence Strategy*, 2020, p. 17). Today's global liberal democratic order faces two challenges. The first is radical Islam – and it is the lesser of the two challenges. Although the proponents of radical Islam find liberal democracy repugnant, and the movement is often described as the new fascist threat, the societies from which it arises are generally poor and stagnant. They represent no viable alternative to modernity and pose no significant military threat to the developed world. It is mainly the potential use of weapons of mass destruction – particularly by non-state actors – that makes militant Islam a menace. The second, more significant, challenge emanates from the rise of nondemocratic great powers: The old Cold War rivals of the West – China and Russia, now operating under authoritarian capitalist, rather than communist, regimes. Authoritarian capitalist great powers played a leading role in the international system up until 1945.

The United States has a strong interest in precluding the emergence of another bipolar world – as in the Cold War – or a world of many great powers, as existed before the two world wars. Multipolarity led to two world wars and bipolarity resulted in a protracted worldwide struggle with the risk of nuclear annihilation. To avoid a return to such circumstances, Secretary of Defense Dick Cheney ultimately agreed that the USA objective must be to prevent a hostile power to dominate a *"critical region"*, which would give it the resources, industrial capabilities and population to pose a global challenge. This insight has guided US defence policy throughout the post-Cold War era (Khalilzad, 2016).

The Cold War era, which is generally viewed as lasting from the late 1940s until the late 1980s or early 1990s, was generally viewed as a strongly bipolar situation featuring two superpowers – the United States and the Soviet Union – engaged in a political, ideological, and military competition for influence across multiple geographic regions. The military component of that competition was often most acutely visible in Europe, where the US-led NATO Alliance and the Soviet-led Warsaw Pact alliance faced off against one another with large numbers of conventional forces and theatre nuclear weapons, backed by longer-ranged strategic nuclear weapons.

The post-Cold War era is generally viewed as having begun in the late 1980s and early 1990s, following the fall of the Berlin Wall in November 1989, the disbanding of the Soviet-led Warsaw Pact military alliance in March 1991, and the dissolution of the Soviet Union into Russia and the former Soviet republics in December 1991, which were key events marking the ending of the Cold War. Compared to the Cold War, the post-Cold War era generally featured reduced levels of overt political, ideological, and military competition among major states.

The post-Cold War era is generally viewed as having tended toward a unipolar situation, with the United States as the world's sole superpower. Neither Russia, China, nor any other country was viewed as posing a significant challenge to either the United States' status as the world's sole superpower or the US-led international order. Following the terrorist attacks of 11 September 2001, the post-Cold War era was additionally characterised by a strong focus (at least from a US perspective) on countering transnational terrorist organisations that had emerged as significant non-state actors, particularly Al Qaeda.

Many observers have concluded that the post-Cold War era began to fade in 2006-2008, and that by 2014 – following Chinese actions in the South and East China Seas and Russia's seizure and annexation of Crimea – when the international environment shifted to a fundamentally different situation of renewed competition for superpower status with China and Russia and due to the challenges of these two countries and other actors to elements of the US-led international order that has operated since World War II (Mearsheimer, 2001, pp. 29-42). Three main sets of challengers – the revisionist powers of China and Russia, the rogue states of Iran and North Korea, and transnational threat organisations, particularly jihadist terrorist groups – are actively competing against the United States and their allies and partners. Although differing in nature and magnitude, these rivals compete across political, economic, and military arenas, and use technology and information to accelerate these contests in order to shift regional balances of power in their favour. These are fundamentally political contests between those who favour repressive systems and those who favour free societies.

John Mearsheimer, scientist and professor of political science at the University of Chicago, defines a great power as a state, having sufficient military assets to put up a serious fight in an all-out conventional war against the dominant power – that would be the United States of America – and possessing a nuclear deterrent that could survive a first strike against it (Work, 2015, p. 3).

China and Russia want to shape a world antithetical to the US values and interests. China seeks to displace the USA in the Indo-Pacific region, expand the reaches of its state-driven economic model, and reorder the region in its favour. Russia seeks to restore its great power status and establish spheres of influence near its borders (Payne et al., 2017, pp. 18-33). The intentions of both nations are not necessarily fixed. The USA stands ready to cooperate across areas of mutual interest with both countries. In addition, after being dismissed as a phenomenon of an earlier century, great power competition returned, China and Russia began to reassert their influence regionally and globally. Today, they are fielding military capabilities designed to deny America access in times of crisis and to contest the ability to operate freely in critical commercial zones during peacetime. In short, they are contesting the geopolitical advantages and trying to change the international order in their favour (National Security Strategy of the United States of America, 2017, pp. 2-3, 25-27).

Today, the United States of America are emerging from a period of strategic atrophy, aware that their competitive military advantage has been eroding. We are facing increased global disorder, characterised by decline in the long-standing rules-based international order – creating a security environment more complex and volatile than any we have experienced in recent memory (Krauthammer, 2014). Inter-state strategic competition, not terrorism, is now the primary concern in US national security.

China is a strategic competitor using predatory economics to intimidate its neighbours while militarising features in the South China Sea. Russia has violated the borders of nearby nations and pursues veto power over the economic, diplomatic, and security decisions of its neighbours (Dibb, 2016, p. 8). As well, North Korea's outlaw actions and reckless rhetoric continue despite the United Nation's censure and sanctions. Iran continues to sow violence and remains the most significant challenge to Middle East stability. Despite the defeat of ISIS's physical caliphate, threats to stability remain as terrorist groups with long reach continue to murder the innocent and threaten peace more broadly (National Defense Strategy of the United States of America, 2018, pp. 1-4).

Challenges to the US military advantage represent another shift in the global security environment. For decades the United States of America has enjoyed uncontested or dominant superiority in every operating domain. In general, they could deploy their forces whenever they wanted, assemble them where they wanted, and operate as they wished. Today, every field is challenged – air, land, naval, space and cyberspace.

The security environment is also affected by the rapid technological advancement and the changing character of war. States are the principal actors on the global stage, but non-state actors also threaten the security environment with increasingly sophisticated capabilities.

KEY CHARACTERISTICS OF DISPUTE REVIVAL

In foreign policy discussions, terms like *unipolar, bipolar, tripolar*, and *multipolar* are sometimes used to refer to the number of top-tier world powers whose actions tend to characterise or give structure to a given historical period's international security situation. The Cold War that lasted from the late 1940s to the late 1980s or early 1990s is usually described as a bipolar situation featuring a competition between two superpowers (the United States and the Soviet Union) and their allies. The post-Cold War era, which followed the Cold War, is sometimes described as the unipolar moment, with the United States being the unipolar power, meaning the world's sole superpower. As mentioned, observers have concluded that in recent years, there has been a shift from the post-Cold War era to a new international security situation characterised by renewed great power competition between the United States, China, and Russia, leading observers to refer to the new situation as a tripolar or multipolar world. Observers who might list additional countries (or groups of countries, such as the European Union) as additional top-tier world powers, along with the United States of America, China, and Russia, might also use the term multipolar.

The term *regional hegemon* generally refers to a country so powerful relative to the other countries in its region that it can dominate the affairs of that region and compel other countries in that region to support (or at least not oppose) the hegemon's key policy goals. The United States of America is generally considered to have established itself in the 19th century as the hegemon of the Western Hemisphere.

Many observers view the new international security environment not as a bipolar situation, like during the Cold War, or as a unipolar situation, like the post-Cold War era, but as a situation largely characterised by renewed competition among the three great world powers – the United States of America, China and Russia. The key features of the current situation of renewal of competition for superpower status include, but are not necessarily limited to, the following:

- the use by Russia and China of new forms of aggressive or assertive military, paramilitary, information, and cyber operations – sometimes called hybrid warfare, grey-zone operations, ambiguous warfare, among other terms, in the case of Russia's actions, and salami-slicing tactics (the process of gradually reducing the size by a series of small incremental steps) or grey-zone warfare, among other terms, in the case of China's actions;
- renewed ideological competition, this time against 21st-century forms of authoritarianism and illiberal democracy in Russia, China, and other countries;
- the promotion by China and Russia through their state-controlled media of nationalistic historical narratives emphasising assertions of prior humiliation or victimisation by Western powers, and the use of those narratives to support revanchist or irredentist foreign policy aims;
- challenges by Russia and China to key elements of the US-led international order, including the principle that force or threat of force should not be used as a routine or first-resort measure for settling disputes between countries, and the principle of freedom of the seas (i.e., that the world's oceans are to be treated as an international commons) (Götz et al., 2019);
- continued regional security challenges from countries such as Iran and North Korea;
- a continued focus – at least from a US perspective – on countering transnational terrorist organisations that have emerged as significant non-state actors – including the Islamic State organisation, among other groups -; and
- weak or failed states, and resulting weakly governed, unpredictable or ungoverned areas that can contribute to the emergence of (or serve as base areas or sanctuaries for) non-state actors, and become potential locations of intervention by stronger states, including major powers.

Evidence of the dispute revival for superpower status. The sharpest single marker of the shift in the international security environment to a situation of renewed great power competition arguably was Russia's seizure and annexation of Crimea in March 2014, which represented the first forcible seizure and annexation of one country's territory by another country in Europe since World War II. Other markers of the shift – such as Russia's actions in eastern Ukraine and elsewhere in Eastern

Europe since March 2014, China's economic growth and military modernisation, as well as, China's actions in the South and East China Seas over the last several years – have been more gradual and cumulative.

The beginnings of the shift from the post-Cold War era to renewed great power competition can be traced to the period 2006-2008:

- Freedom House's annual report on freedom in the world for 2019 states, by the organisation's own analysis, that countries experiencing net declines in freedom have outnumbered countries experiencing net increases in freedom for 13 years in a row, starting in 2006 (Freedom House, 2019, p. 5);
- in February 2007, in a speech at an international security conference in Munich, Russian President Vladimir Putin criticised and rejected the concept of a unipolar power, predicted a shift to multipolar order, and affirmed an active Russian role in international affairs. Some observers view the speech in retrospect as prefiguring a more assertive and competitive Russian foreign policy (Rumer, pp. 10-12);
- in 2008, Russia invaded and occupied part of the former Soviet Republic of Georgia without provoking a strong cost-imposing response from the USA and its allies (Rice, 2018). Also in that year, the financial crisis and resulting deep recessions in the USA and Europe, combined with China's ability to weather that crisis and its successful staging of the 2008 Summer Olympics, are seen by observers as having contributed to a perception in China of the United States of America as a declining power, and to a Chinese sense of self-confidence or triumphalism (Broderick, 2015, pp. 2, 4, 6-10). China's assertive actions in the South and East China Seas can be viewed as having begun or accelerated soon thereafter.

Other observers trace the roots of the shift to renewed great power competition further, to years prior to 2006-2008 (Blustein, 2019).

Comparison to past international security environments. Some observers seek to better understand the current situation of renewed competition for superpower status in part by comparing it to past international security environments. Each international security environment features its own combination of major actors, dimensions of competition and cooperation among those actors, and military and other technologies available to them. A given international security environment can have some similarities to previous ones, but it will also have differences, including, potentially, one or more features not present in any other international security environment. In the early years of a new international security environment, some of its features may be unclear, in dispute, not yet apparent, or subject to evolution. In attempting to understand an international security environment, comparisons to other ones are potentially helpful in identifying avenues of investigation. If applied too rigidly, however, such comparisons can act as intellectual straightjackets, making it more difficult to achieve a full understanding of a given international security environment's characteristic features, particularly those that differentiate it from previous ones.

Some observers have stated that the world has entered a new Cold War (or Cold War II or 2.0). That term may have some utility in referring specifically to US-Russian or US-Chinese relations, because the era of renewed great power competition features rivalry and tension with Russia and China. Considered more broadly, however, the Cold War was a bipolar situation with the United States of America and Russia, while the era of renewed great power competition is a situation that also includes China as a major competing power (Gareis, 2019). The bipolarity of the Cold War, moreover, was reinforced by the opposing NATO and Warsaw Pact alliances, whereas in contrast, Russia and China today do not lead an equivalent of the Warsaw Pact. And while terrorists were a concern during the Cold War, the USA focused on countering transnational terrorist groups but it was not nearly as significant during the Cold War as it has been since 9/11. Other observers, viewing the renewal of great power competition, have drawn comparisons to the multipolar situation that existed in the 19th century and the years prior to World War I. Still others, observing the promotion in China and Russia of nationalistic historical narratives supporting revanchist or irredentist foreign policy aims, have drawn comparisons to the 1930s (Gotz, pp. 135-137).

Those two earlier situations, however, did not feature a strong focus on countering globally significant transnational terrorist groups, and the military and other technologies available then differ vastly from those available today. The current period of renewed great power competition may be similar in some respects to previous situations, but it also differs from previous situations in certain respects, and might be best understood by direct observation and identification of its key features. Observers viewing the international security environment have given it various names, but names using some variation of great power competition or renewed great power competition appear to have become most commonly used in public policy discussion. Other terms that have been used include *competitive world order, multipolar era, tripolar era, and disorderly world (or era)*.

The previous major change in the international security environment – the shift in the late 1980s and early 1990s from the Cold War to the post-Cold War era – prompted a broad reassessment by the DOD and Congress of defence funding levels, strategy, and missions that led to numerous changes in DOD plans and programmes. Many of the mentioned changes were articulated in the 1993 *Bottom-Up Review (BUR)* (Report on the Bottom-Up Review, 1993, pp. 71-107), a reassessment of US defence plans and programmes whose very name conveyed the fundamental nature of the re-examination that had occurred. In general, the BUR reshaped the US military into a force that was smaller than the Cold War US military, and oriented toward a planning scenario being able to conduct two major regional contingencies rather than the Cold War planning scenario of a NATO-Warsaw Pact conflict.

In March 1993, it was initiated a comprehensive review of the US defence strategy, force structure, modernisation, infrastructure, and foundations. It was considered that a department-wide review needed to be conducted *"from the bottom up"* because of the dramatic changes that had occurred in the world as a result of the end of the Cold War and the dissolution of the Soviet Union. These changes in the international security environment have fundamentally altered America's security needs. Thus, the underlying premise of the Bottom-Up Review was that it needed to reassess all defence concepts, plans, and programmes from the ground up.

US ROLE IN THE WORLD

While descriptions of the US purpose in the world since the end of World War II vary in their specifics, it can be described in general terms as consisting of four key elements: global leadership; defence and promotion of the liberal international order; defence and promotion of freedom, democracy, and human rights; and prevention of the emergence of regional hegemons in Eurasia (Kagan, 2017, p. 1). The issue is whether the US role in the world is changing, and if so, what implications this might have for the United States of America and the world. This could significantly affect the US policy in areas such as relations with allies and other countries, defence plans and programmes, trade and international finance, foreign assistance, and human rights.

Some observers view the change as an unnecessary retreat from US global leadership and a gratuitous discarding of long-held western values, and judge it to be an unforced error of immense proportions – a needless and self-defeating squandering of something of great value to the United States of America that it had worked to build and maintain for 70 years.

Other observers who assess that there has been a change in the US role in the world in recent years as well as some observers who argue in favour of a more restrained US role in the world view the change in the US role, or at least certain aspects of it, as helpful for responding to changed US and global circumstances and for defending US values and interests, particularly in terms of adjusting the US role to one that is more realistic regarding what the United States of America can accomplish, enhancing deterrence of potential regional aggression by making potential US actions less predictable to potential adversaries, re-establishing respect for national sovereignty as a guidepost for US foreign policy and for organising international affairs, and encouraging US allies and security partners in Eurasia to do more to defend themselves.

A fourth element of the US role in the world since World War II – one that US policymakers do not often state explicitly in public – has been to oppose the emergence of regional hegemons in Eurasia. This objective reflects a US perspective on geopolitics and grand strategy developed by US strategists and policymakers during and in the years immediately after World War II that incorporates two key judgments:

- first, that given the amount of people, resources, and economic activity in Eurasia, a regional hegemon in Eurasia would represent a concentration of power large enough to be able to threaten vital US interests;
- second, Eurasia is not dependably self-regulating in terms of preventing the emergence of regional hegemons, meaning that the countries of Eurasia cannot be counted on to be able to prevent, though their own actions, the emergence of regional hegemons, and may need assistance from one or more countries outside Eurasia to be able to do this dependably (National Defense Strategy of the USA, pp. 1-11).

Preventing the emergence of regional hegemons in Eurasia is sometimes also referred to as preserving a division of power in Eurasia, or as preventing key regions in Eurasia from coming under the domination of a single power, or as preventing the emergence of a spheres-of-influence world, which could be a consequence of the emergence of one or more regional hegemons in Eurasia.

US actions that can be viewed as expressions of the US goal of preventing the emergence of regional hegemons in Eurasia include but are not necessarily limited to the following:

1. US participation in World War I, World War II, the Korean War, and the Vietnam War;

2. US alliances and security partnerships, including:

a) NATO Alliance, which was established in large part to deter and counter attempts by the Soviet Union (now Russia) to become a regional hegemon in Europe;

b) US alliances with countries in East Asia and the Pacific, which were established in large part to deter and counter attempts by the Soviet Union or China to become a regional hegemon in East Asia; and

c) US security partnerships with countries in the Persian Gulf region, which were established in large part to deter or counter attempts by Iran or the Soviet Union (now Russia) to become a regional hegemon in that region; and

3. additional US political, diplomatic, and economic actions to contain and oppose the Soviet Union during the Cold War, including the Marshall Plan and subsequent US foreign assistance programmes.

In pursuing the goal of preventing the emergence of regional hegemons in Eurasia, US policymakers have sometimes decided to work with or support nondemocratic regimes that for their own reasons view Russia, China, or Iran as competitors or adversaries. As a consequence, the goal of preventing the emergence of regional hegemons in Asia has sometimes been in tension with defending and promoting freedom, democracy, and human rights.

POTENTIAL IMPACT OF COVID-19 (CORONAVIRUS)

For the first time in the 21st century, the world is facing a pandemic that has affected all states and triggered an economic crisis that will affect the serious power relations between global actors, which will increase the volatility and unpredictability, already accentuated, of the international security environment. A rapidly emerging but potentially very significant issue is the question of whether and how the global COVID-19 pandemic might lead to profoundly transformative and long-lasting changes in both the structure of international politics and the US role in the world in areas such as US global leadership, China and Russia's potential for acting as a global leader, US strategic competition with China and Russia, US relations with allies, and US definitions of US national security.

Some observers argue the COVID-19 pandemic could be a world-changing event with potentially profound and long-lasting implications for the international security environment and the US role in the world. Other observers are more sceptical that the COVID-19 pandemic will have such effects.

Observers who argue the COVID-19 pandemic could be world-changing for the international security environment and the US role in the world have focused on several areas of potential change, including the following, which are listed here separately but overlap in some cases and can interact with one another:

- world order, international institutions, and global governance;
- US global leadership and the US role in the world;
- China and Russia's potential role as a global leader;
- US relations and great power competition with China and Russia, including the use of the COVID-19 pandemic as a theme or tool for conducting ideological competition;
- the relative prevalence of democratic and authoritarian or autocratic forms of government;
- societal tension, reform, transformation, and governmental stability in various countries;
- the world economy, globalisation, and US and China trade policy;
- the characteristics and conduct of conflict;
- allied defence budgets and US alliances, as well as those of Russia and China;
- the cohesion of the European Union;
- the definition of, and budgeting for US national security as well as Russia and China;
- USA, Russia and China defence strategies, defence budgets, and military operations;
- US foreign assistance programmes and international debt relief;
- activities of non-state actors;
- the amount of US, Russia and China attention devoted to ongoing international issues other than the COVID-19 pandemic.

Some observers have focused on how, in their view, the COVID-19 pandemic is demonstrating that the United States of America is maintaining or reasserting its role as a global leader, while other observers suggest that, the COVID-19 pandemic is demonstrating that the United States of America has chosen to withdraw from or is no longer capable of performing that role. The COVID-19 pandemic could influence discussions over the costs and benefits to the USA of acting as a global leader, not only with respect to global health but across a range of issues. Some analysts have focused on how the COVID-19 pandemic may be providing insight into whether China and Russia desire and work to become a global leader on par with (or in the place of) the United States of America, whether China and Russia have a capacity for doing so, and how other countries might view them acting in such a role.

China's transparency, particularly regarding its actions in the early days of its COVID-19 outbreak in Wuhan, as well as China's so-called donation diplomacy or mask diplomacy – meaning China's actions to send medical supplies and personnel to other countries, and the highlighting of these actions in statements from China's government and state controlled media – have become new elements of an ongoing discussion regarding China's capacity or suitability for acting as a global leader.

This ongoing discussion includes consideration of a range of other issues, including China's actions for implementing its Belt and Road Initiative, China's territorial disputes with other countries, its participation in international organisations, and its technology-development and international lending activities. Some observers have focused on how the COVID-19 pandemic has become a significant element in USA-China relations, and in US great power competition with China and Russia.

For some observers, the COVID-19 pandemic presents an opportunity for USA-China cooperation on an important international issue of common interest. For other observers, the COVID-19 pandemic is a major new source of dispute and arena of competition between the two countries, and it is causing USA-China relations to harden more fully into a Cold War-like adversarial situation.

Some observers have focused on how the COVID-19 pandemic provides a prominent new factor in the discussion of whether the United States of America should decouple its economy from China's and reduce its dependence on China for key materials and products, including hospital supplies and pharmaceuticals.

Some observers have focused on whether the US and Chinse responses to the COVID-19 pandemic will affect views around the world regarding the relative merits of the US and Chinese forms of government and economic models as potential examples to emulate.

CONCLUSIONS

In recent years, the US-led liberal world order that emerged after the end of the Cold War has been shaken. In many ways, though, what has emerged as the most immediate challenge to the current international order is Russia's increasingly proactive and assertive behaviour.

There is broad agreement among commentators and analysts that Russia seeks to undermine the US-led liberal international order. At the same time, there is considerable disagreement over the nature and extent of the challenge Moscow poses, the underlying drivers of Russian revisionism, and how the West should respond.

It is possible to distinguish between three major perspectives. In brief, the first suggests that Russia is a *"revanchist power"* that seeks to overturn the very foundations of the liberal world order. The second perspective holds that Russia is a *"defensive power"* that works for incremental changes within the existing order. The third perspective contends that Russia is an *"aggressive isolationist"*, meaning that the Putin regime deliberately plays a spoiler role in international affairs to boost its domestic legitimacy. Moscow's revisionist agenda manifests itself in several ways. First, Russia challenges established rules and norms in the post-Soviet space, including the sanctity of international borders. The takeover of Crimea, in this perspective, was only the latest, and most extreme, example of a much broader pattern of behaviour. Over the course of the past decade, Russia has gone to war with Georgia; repeatedly interfered in the domestic political affairs of neighbouring countries; exerted various forms of economic pressure on states like Ukraine, Moldova, and Lithuania; and expanded its network of military bases in the post-Soviet region. The ultimate goal of these activities is to establish an exclusive sphere of influence on the territory of the former Soviet Union. In other words, the grand ambition is to undo the post-Cold War settlement to re-establish Russia as a dominant power in Eurasia. Second, Russia seeks to exploit the West's openness and vulnerabilities – information systems, political pluralism, and socio-economic fault lines – to create divisions within the Euro-Atlantic community. Third, Moscow is forging alliances with likeminded authoritarian regimes in countries such as Belarus, Iran, Syria, Venezuela, and, most importantly, China. China and Russia together, represent the core of a new coalition of anti-democratic autocracies challenging the Western-imposed, post-Cold War status quo.

In an international security environment described as one of renewed super power competition, the South China Sea has emerged as an arena of USA-China strategic competition. China's actions in the South China Sea in recent years – including extensive island-building and base construction activities at sites that it occupies in the Spratly Islands, as well as actions by its maritime forces to assert China's claims against competing claims by regional neighbours such as the Philippines and Vietnam – have heightened concerns among US observers that China is gaining effective control of the South China Sea, an area of strategic, political, and economic importance to the United States of America and its allies and partners. Actions by China's maritime forces at the Japan administered Senkaku Islands in the East China Sea are another concern for the USA. Chinese domination of China's near-seas region – meaning the South China Sea and East China Sea, along with the Yellow Sea – could substantially affect US strategic, political, and economic interests in the Indo-Pacific region and elsewhere.

Summarising, there are three main sets of challengers – the revisionist powers of China and Russia, the rogue states of Iran and North Korea, and transnational threat organisations, particularly jihadist terrorist groups – that are actively competing against the United States of America and its allies and partners.

BIBLIOGRAPHY:

1. Blustein, P. (2019). *"The Untold Story of How George W. Bush Lost China"*. In Foreign Policy, https://foreignpolicy.com/2019/10/04/the-untold-story-of-how-george-w-bush-lost-china/, retrieved on 4 September 2020.
2. Broderick, K. (2015). *"Chinese Activities in the South China Sea, Implications for the American Pivot to Asia"*. In Project institute 2049, https://project2049.net/wp-content/uploads/2018/06/150511_Broderick_Chinese_Activities_South_China_Sea_Pivot.pdf, retrieved on 4 September 2020.
3. Dibb, P. (2016). *"Why Russia is a threat to the international order?"*. In Strategy, The Australian Strategic Policy Institute, https://s3-ap-southeast-2.amazonaws.com/ad-aspi/import/Russia.pdf?pIMhBAf0i_aHd1.6Y_Jx3ZGEq547f3yB, retrieved on 2 September 2020.
4. Gareis, B.S. (2019). *"Taking off as a Global Power? China's Foreign Policy"*. In Grand Strategy, Marshall Center/Occasional Papers, https://www.marshallcenter.org/sites/default/files/files/2019-07/PDF_PUB_OPS_24.pdf, retrieved on 4 September 2020.
5. Götz, E., Merlen, C.-R. (2018). *"Russia and the question of world order"*. In Russia and the question of world order, European Politics and Society, vol. 20, No. 2, https://www.tandfonline.com/doi/pdf/10.1080/23745118.2018.1545181?needAccess=true, retrieved on 2 September 2020.
6. Kagan, R. (2017). *"Backing into World War III"*. In Foreign Policy, https://foreignpolicy.com/2017/02/06/backing-into-world-war-iii-russia-china-trump-obama/, retrieved on 2 September 2020.
7. Khalilzad, Z. (2016). *"4 Lessons about America's Role in the World"*. In National Interest, https://nationalinterest.org/feature/4-lessons-about-americas-role-the-world-15574, retrieved on 2 September 2020.
8. Krauthammer, C. (2014). *"Who made the pivot to Asia? Putin"*. In The Washington Post, https://www.washingtonpost.com/opinions/charles-krauthammer-who-made-the-pivot-to-asia-putin/2014/05/22/091a48ee-e1e3-11e3-9743-bb9b59cde7b9_story.html?utm_term=. 1a39f00406c7, retrieved on 2 September 2020.
9. Mearsheimer, J.J. (2001). *"The tragedy of great power politics"*. New York and London: W.W. Norton & Company, https://edisciplinas.usp.br/pluginfile.php/5526008/course/section/6018533/MEARSHEIMER%20J.%20%282001%29.%20The%20Tragedy%20of%20Great%20Power%20Politics%20-%20Cap%202.pdf, retrieved on 2 September 2020.

10. Payne, K.B., Foster, J.S. (2017). *"Russian strategy: Expansion, crisis and conflict".* In Comparative Strategy, 36(1), 1-89, https://www.tandfonline.com/doi/abs/10.1080/01495933.2017.1277121, retrieved on 2 September 2020.
11. Rice, C. (2018). *"Russia Invaded Georgia 10 Years Ago. Don't Say America Didn't Respond".* In Washington Post, https://www.washingtonpost.com/opinions/russia-invaded-georgia-10-years-ago-dont-say-america-didnt-respond/2018/08/08/ba4279d4-9b3e-11e8-8d5e-c6c594024954_story.html, retrieved on 2 September 2020.
12. Rumer, E. *"Russia and the security of Europe"*. In Carnegie endowment for international peace, https://carnegieendowment.org/files/CP_276_Rumer_Russia_Final.pdf , retrieved on 2 September 2020.
13. Work, B. (2015). Deputy Secretary of Defense Speech. In *U.S. Department of Defense*, CNAS Defense Forum, JW Marriott, Washington, D.C., https://www. defense.gov/Newsroom/Speeches/Speech/Article/634214/cnas-defense-forum/, retrieved on 5 September 2020.
14. Presidential Administration. *National Defence Strategy for the period 2020-2024*. (2020). București: Monitorul Oficial, Part I, no. 574 on 1 July 2020.
15. Office of the President. *National Security Strategy of the United States of America*. (2017), https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf, retrieved on 2 September 2020.
16. Department of Defense. *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge.* (2018), https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf, retrieved on 25 September 2020.
17. Department of Defense, *Report on the Bottom-Up Review, Les Aspin, Secretary of Defense*. (1993), https://www.hsdl.org/?view&did=448259, retrieved on 8 August 2020.
18. *Freedom in the World 2019* (2019). Freedom House, https://freedomhouse.org/sites/default/files/Feb2019_FH_FITW_2019_Report_ForWeb-compressed.pdf, retrieved on 9 September 2020.
19. Stanford Global Studies (2018), https://medium.com/stanford-global-perspectives/the-decline-of-u-s-hegemony-in-the-western-hemisfere-b1015a4b636e, accesat la 11 septembrie2020.

THE IMPACT OF THE SECURITY ENVIRONMENT ON THE DEFENCE STRATEGIES OF SMALL AND MEDIUM STATES

Teacher Ioana RIEBER, PhD

"Gheorghe Lazăr" National College, Bucharest

The dynamic of regional and global changes implies the existence of strategies that allow the streamlining of the activity of defence and security structures. Depending on the risks, vulnerabilities and threats that must be approached militarily or non-militarily, the medium and small states have drafted strategic documents, taking into account the internal and external dimension of security. Their security depends on a great extent on external factors, the turbulences from the international system posing a serious challenge for a small state.

If small and medium states are placed in the vicinity of a great revisionist, undemocratic power, its security can be achieved only by creative strategies. The emphasis is therefore laid on the existence of flexible and powerful military capabilities, necessary to identify and counter the threats and on membership of alliances/coalitions of alliances.

Keywords: small and medium powers; alliances; strategic documents; integration; security; military capabilities;

INTRODUCTION

The world has never been safe for states considered to be small and medium powers because they cannot afford a high-intensity conflict with a great power, which is why they are forced to think about their defence strategy to ensure their security by using their material and human resources with maximum efficiency. The means and methods small and medium states use are varied, from diplomacy, bilateral, and multilateral relations to military alliances, or asking support from international organisations, as collective security bodies.

TYPES OF SECURITY STRATEGIES USED BY SMALL AND MEDIUM STATES

A small or medium state cannot play a decisive role in international relations and cannot change the rules of the world because, first of all, its quantitative characteristics, such as the small size of the territory, population, economy or the very limited military capabilities, do not allow this.

Political Science Professor Baldur Thorhallsson used six criteria that must be taken into account in the classification of a state in a certain category of power (2018, pp.17-34): (1) absolute size [population and territory]; (2) economic size [namely, GDP, market size, development success]; (3) sovereignty dimension [whether the state can maintain effective sovereignty on its territory], (4) political size [military and administrative capabilities and the degree of domestic cohesion, combined with the degree to which the state maintains a united external front]; (5) perceptual size [political discourse, self-identity]; and (6) preference size [ambitions and prioritisations of the governing elite]. Although it has an inward-looking, Thorhallsson's schematic framework is relevant to the analysis of the state's capacity and insecurity in implementing national security policy and strategy (Domingo-Almase, 2019).

The level of military capabilities as well as a strong economy are significant factors that define the challenges and limitations of small states, but insufficient to explain their foreign policies. Historical background, geographical position or social-political practices are also important in states' classification.

The medium states can be regional actors to be taken into account; for example, Denmark is a small NATO state, but a powerful actor in relation to the Baltic States. The strategic environment makes the security agendas of small states to be personalised, as they are located in different geographical areas with different neighbours and face different problems. Depending on the effectiveness of decisions made by political factors, their territory size does not prevent small states from being active or influencing international relations, they can participate in military operations, such as Sweden, Finland and Denmark, or they can make important contributions to solving contemporary world issues, thus exerting a certain influence within international organisations (Vaicekauskaitė, 2017, pp. 7-15).

The basic tools of a small state are foreign policy and diplomacy. Diplomacy is the first line of defence in international conflicts. Underdeveloped states often have to develop the most complex diplomatic repertoires to counter the movements of much larger states. As a rule, the *"guiding star"* of the foreign policies of small states has been defence, not attack, but there are of course exceptions, such as Israel and Cuba (Maniruzzaman, 1982).

States choose policies that best reflect their interests, either a more passive and neutral role or active engagement. Increasing influence does not always lead to an increase in security ratio. They need a peaceful international system and security guarantees from strong states or organisations. The common security and defence project was the idea of the great European states, but the goal of being well-positioned in the international system was the main reason that forced almost all small states to join. The difference between states that managed to survive and those that perished is that some small states survived because of their commitments, which led them to the a chievement of their desired goal, that of preserving security.

Alliances can be bilateral or multilateral; they can include small and large powers. The advantage of the alliance is that of military support of the allies in case of need. There is a situation when a small state could obtain the protection of a great ally: when the first can serve the power interests of the latter. The best examples in this regard are Israel, protected by the USA, interested in the Middle East and also Cuba, protected by the Soviet Union, interested in the USA. Alliances usually bring together members with similar strategic interests and ideologies. Modern alliances such as NATO are highly institutionalised with a formal collective commitment to defend their member countries.

Joining alliances can also have disadvantages. For example, the Soviet Union invaded Afghanistan in 1979 at the invitation of Babrak Kamal under the Treaty of Friendship, Good Neighbourhood and Cooperation, signed in 1978. Also, in the framework of multilateral and bilateral treaties signed with the majority of its former colonies, France often brought about changes of government in these countries, by intervening in Cameroon, Congo, Chad, Niger, Mauritania, in Gabon in 1964, and the Central African Republic in 1967; thus, the alliance functioned as a double-edged sword.

Another problem would be that the great powers play a huge role in managing the risks in small states, as they provide them with additional resources, military capabilities and political support, but in exchange for protection, they can limit their freedom. There is another strategic option that states can use to increase their security: entering regional alliances. On the one hand, India has concluded defence treaties with its neighbours – Bhutan, Nepal, and Bangladesh – to protect them from the influences of foreign powers, especially China. China, on the other hand, has entered into a non-aggression pact with two of its neighbours – Burma and Afghanistan – to prevent them from joining an alliance with India in the event of a Sino-Indian military confrontation. Also, the Arab states formed two successive alliances to fight Zionism and fight Israel.

In this concern, there are several strategies that small states use: they can align with the states that threaten them, voluntarily subordinating themselves to a great power to obtain more protection and public order, increased security and territorial integrity, or they can ally with other powers against a potential aggressor, to obtain higher levels of security. Alignment can stimulate the political regimes weakening or, on the contrary, increase their resilience; therefore, there are weaker states where internal instability motivates the political elite to align with stronger countries seeking to improve their internal stability (Vaicekauskaitė, Ibid).

Small and medium states can use strategic coverage when they do not want to support a party or a power, fearing that this could lead to higher security risks. This strategy falls between balancing and bandwagoning[1]. A practical example of implementing such a strategy could be the case of Southeast Asian countries, which, due to the direct influence of the USA and China, prefer this security strategy option. This type of policy is about misalignment and has been used often by third world states.

Another strategy is neutrality in the event of a conflict. From a legal perspective, neutral states are required not to take part in wars, and not to be part of military alliances or to support militarily a state involved in that conflict. To respect neutrality, the geographical position counts because its neutral position would be strategically advantageous to the major powers or not prevent them from achieving their objectives. For this situation, one must see the case of Belgium, whose neutrality was violated by Germany in 1914 and 1940, to enter in France with troops, although the two powers have a common border.

[1] In international relations, bandwagoning occurs when a state aligns with a stronger, adversarial power and concedes that the stronger adversary-turned-partner disproportionately gains in the spoils they conquer together (https://www.thefreedictionary.com/bandwagoning).

The disadvantage of the neutral state is that it should be ready to defend itself in the event of a violation of territorial integrity or sovereignty. Switzerland has chosen to remain neutral and formally to pursue this policy even today. Yet it has sought to be active in international affairs, supporting peace-building operations of security organizations and becoming a centre for associations working to manage a crisis in the world.

The third world states find Swiss-style neutrality particularly attractive. For example, Prince Sihanouk of Cambodia, Sheikh Mujibur Rahman of Bangladesh and King Birendra of Nepal, all expressed a desire to turn their countries into the *"Switzerland of Asia"*. However, neutrality in the international community is easier to desire than to achieve (Ibid).

Small states need different capabilities to address the complexity of the security challenges they face. This requires collaboration with various actors and security providers to mitigate the risks. Beyond military alliances, there are strong international organisations: worldwide, the UN aims to maintain peace, being a guarantor of the security of small and medium states, at the regional level, for the Middle East and Africa there are the Organization of Islamic States, the African Union, etc.

BRIEF STUDY CASES – SMALL STATES SECURITY

If one analyses the example of the Baltic States can see that their security depend largely on external factors. Lithuania, Latvia and Estonia are located in a common operational environment, which faces a similar set of security threats and challenges. These challenges are largely related to Russia's dominance in the region and its assertive growth actions. To survive, they used different tools and strategies.

After regaining independence, Lithuania, Latvia and Estonia chose not to run out of alliances, seeking to integrate into the Euro-Atlantic institutions, namely NATO and the EU, to cooperate with the USA, while trying to intensify trilateral defence cooperation. (BALTBAT, BALTRON, BALTNET) (Baltic Defence Co-operation, 2014) and look for common solutions on how to strengthen their defence capabilities. After 2014, in the face of growing tensions in the region, the three Baltic States began to readjust their security policies, focusing on strengthening their national defence capabilities. For the small states of the Western Balkans, there is only one strategic choice, namely Euro-Atlantic integration.

A weak army and a corrupt bureaucracy make the Philippines small and vulnerable to internal and external threats. The Philippines are struggling to patrol their vast expanse of water due to a lack of equipment and resources generated by limited border security and lack of defence funding. Thus, in an apparent move to compensate for this weakness, there are plans to strengthen cooperation and a peaceful approach with countries sharing common borders and maritime interests, to strengthen alliances, to develop new security agreements and to expand commitments with regional and international institutions. Security mentality and political orientation (e.g. nation-building, economic pragmatism, internally oriented armed forces, and institutional shelter), that are typical for a small state (Domingo-Almase, Ibid).

Third world nations (Egypt, India, Indonesia and Iran for example) have pursued an outward orientated *"active strategy"*, and an expansive foreign policy, aiming to assert their national identity and existence in the international arena. In this direction, Nasser used propaganda, Arab nationalism, subversion, and increased armed forces. As a result, Egypt's prestige has grown in the international arena.

Indonesia under Sukarno pursued a *"policy of confrontation"* with Malaysia and the Indonesian armed forces *"liberated"* West Irian. Sukarno's successors pursued a less aggressive foreign policy but did not miss the opportunity to annex East Timor. Still, in 1999, under UN pressure, Indonesia gave up Timor, which in 2002 became an independent state.

Nepal is an underdeveloped country occupying a dangerous geopolitical place between two giants, India and China. Its relations with India were contradictory: India invested in its economy but was also a refuge for Nepalese opposition leaders. Things began to change when Mahendra ascended the throne of Nepal in 1955 and brought the Chinese factor to the Himalayas for the first time, as a potential counterbalance to India, by appointing pro-Chinese or pro-Indian politicians as prime ministers considering political interests. He launched a new policy of *"non-alignment with equal friendship"* (meaning the end of the special relationship with India), being signed the first trade and aid agreement with China, implemented by an anti-Indian prime minister (Maniruzzaman, Ibid). However, eighteen months later, Mahendra replaced for a short time the pro-Chinese prime minister with another to protect India. But, the newly appointed pro-Indian went too close to India and the king dismissed him only three months after his appointment. The president took over the administration and added a new dimension to its balance by concluding an aid agreement with the Soviet Union. His measures proved their efficiency: in 1955, when he came to the throne, Nepal had diplomatic relations with only five countries and, by 1959, it had been recognised by 24 governments and admitted to the United Nations. In 1968, Nepal was elected in the Security Council as a non-permanent member.

In the Cold War era, Romania was part of the Council for Mutual Economic Assistance but opposed supranational planning. It had the foreign trade oriented to the west and also had economic treaties with Mongolia, Cuba, China etc. Romania followed the idea of a nation-state that had the right to decide on its foreign policy. While Moscow campaigned for the subordination of national interests to the interests of the communist community, Bucharest maintained an independent line from Moscow and had a more nuanced position vis-à-vis the member states of the Warsaw Pact (Stephen, 1984). Nicolae Ceaușescu maintained a good relationship with the USA, interested in the geopolitical settlement of Romania and with the Popular Republic of China, thus managing to avoid the USSR invasion in Romania in 1968.

In the morning of 21 August 1968, Soviet, Hungarian, Polish, East German and Bulgarian troops entered into Czechoslovakia at the USSR request. In the same day, in the afternoon, Nicolae Ceaușescu addressed the people gathered in front of the headquarters of the Central Committee of Romanian Communist Party blaming the invasion. When he opposed to an action decided by Moscow, the president hoped for the USSR rival states, China, USA and Yugoslavia, to support Romania. His expectations were justified as, on 23 August 1968, at the reception organised for the National Day in the Romanian Embassy in Beijing, the Chinese Prime Minister Zhou Enlai affirmed Romania in fighting for its defence could count on the Chinese people support (Tomozei, 2016). On his turn, in response to the Romanian diplomat Corneliu Mănescu, US President Lyndon Johnson sent a message to the Soviets: *"Do not let slip the dogs of war!"* (Betea, 2009, p. 59). On 24 August, Ceausescu met with Tito in the locality near the Vârşeţ border where Tito assured him that he could withdraw to Yugoslav territory at any time. It was also discussed the possibility to form an eventual common defence front against Moscow.

At the end of August 1968, Ceauşescu's situation was complicated. According to the Intelligence Service data, 235,000 soldiers belonging to the Odessa, Lviv and Kyiv Commands had been deployed on Romania's borders with the Soviet Union (Marcu, Ibid). Also, naval ships of the Soviet fleet were stationed near the mouths of the Danube and the Romanian Black Sea coast. In this context, Dean Rusk, the head of the USA State Department, handed a note to Anatoli Dorinin, the Soviet ambassador to Washington, asking him not to invade Romania, as the consequences would be unpredictable (Betea, Ibid., p. 60).

Measures were taken to resist a possible Soviet invasion: the Romanian Armed Forces were mobilised, the Patriotic Guards were established, the law on *Preparing Youth for the Defence of the Motherland* was voted, introducing the obligation to attend military training courses for all students, Also, on 23 August, Ceaușescu met with two high-ranking Czechoslovak activists to form a possible common defence front against Moscow. The security analysed how the invasion of Czechoslovakia had taken place to cancel the possibility of repeating such a scenario in Romania as well. Airports were placed under strict guard, and the number of Soviet tourists was closely

monitored. The refusal of the Romanian authorities to allow military operations on its territory made difficult a scenario similar to the one applied in Czechoslovakia (Watts, 2011, p. 379). Romania has continued the path of independence in foreign relations and it is often suggested that it could serve as a model of *modus vivendi* between a superpower and a lower power. Romania has obtained a substantial autonomy in foreign relations, was surrounded by communist states.

The role of small and medium states in international relations is unjustly little studied. However, according to certain experts in the field, the conclusion was reached that small states generally choose multilateralism for two reasons: as a way to influence and as a means to limit bigger states. A small state is capable of developing priorities and use the strategies of a coalition it is part of to build its image.

We cannot fail to notice that states able to reach their foreign policy objectives benefit from a well-thought and sometimes even courageous security strategy.

BIBLIOGRAPHY:

1. Betea, L. (coord.). (2009). *21 august 1968. Apoteoza lui Ceaușescu*. Iași: Editura Polirom.
2. Domingo-Almase, *D.A. Small Sate Security Syndrome: Understanding the Philippines'*. National Security Strategy, https://theasiadialogue.com/2019/02/19/the-long-read-small-state-security-syndrome-understanding-the-philippines-national-security-strategy/, retrieved on 2 August 2020.
3. Gashi, B. *Small States and National Security*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2818984, retrieved on 2 August 2020.
4. Larrabee, S. (1984). *The Challenge to Soviet Interests in Eastern Europe: Romania*, Hungary, East Germany. Santa Monica, CA: RAND Corporation, https://www.rand.org/pubs/reports/R3190.html., retrieved on 12 September 2020.
5. Maniruzzaman, T. (1982). *The Security of Small States in the Third World*. The Strategic and Defence Studies Centre. The Research School of Pacific Studies The Australian National University Canberra, Australia and London, England and Miami, Florida, USA, http://bellschool.anu.edu.au/sites/default/files/publications/attachments/2016-03/sdsc-maniruzzaman.pdf., retrieved on 2 August 2020.
6. Marcu, I. (2018). *A fost România aproape de o invazie sovietică în 1968?* În Historia", https://www.historia.ro/sectiune/general/articol/a-fost-romania-aproape-de-o-invazie-sovietica-in-1968, retrieved on 2 August 2020.
7. Thorhallsson, B. (2018). *Studying Small States: A Review*. In "Small States & Territories". Vol. 1, no. 1, https://www.researchgate.net/publication/327074818_Studying_small_states_A_review, retrieved on 24 October 2020.
8. Tomozei, D. (2016). *Statul în secolul XXI – modelul chinez*. Editura Corint, http://romanian.cri.cn/221/2017/08/29/1s181435.htm, retrieved on 24 October 2020.
9. Vaicekauskaitė, Ž.M. (2017). *Security Strategies of Small States*. In "Changing World Journal on Baltic Security", retrieved on 2 August 2020.
10. Watts, L.L. (2011). *Fereşte-mă, Doamne, de prieteni. Războiul clandestin al blocului sovietic cu România*. București: Editura RAO.
11. Baltic Defence Co-operation, 2014, https://www.mfa.gov.lv/en/security-policy/co-operation-with-nato-member-states-and-candidate-countries/baltic-defence-co-operation-main-joint-projects, retrieved on 2 August 2020.

WARFARE GENERATIONS. CONVENTIONAL AND UNCONVENTIONAL IN WARFARE EVOLUTION

Lieutenant Cosmina-Andreea NECULCEA

Air Force Academy „Henri Coandă” Braşov

The current article highlights the evolution of warfare generations and how the conventional/ unconventional relationship has changed over time. Looking from this perspective, for the time being, no paradigm allows a complete comparative analysis of the armed confrontations. As the humankind has evolved, the conflict has known a continuous evolution, the nature of warfare being in a perpetual transformation and adaptation to the evolution of technology.

The change consists of the fact that the quantitative dimension has decreased in importance, in relation to the qualitative dimension, and information has taken the place of firepower. The information field has become the main battlefield, and remote actions, without direct contact, have become the main means of achieving objectives. In this article, the evolution of warfare is presented in several distinct phases, also called generations. Therefore, each age corresponds to a warfare generation, grouped based on certain common features.

Keywords: generations; conventional; unconventional; evolution; change;

INTRODUCTION

Over time, warfare has known different forms of materialisation; wars have been classified into different typologies, forms of manifestation and ways of being approached. The purpose of this article is to analyse one of these approaches, namely, the generational one.

Once scientists have accepted the notion of *“warfare generation”*, it is obvious that other generations would continue to appear, in one form or another, at a certain rate of recurrence, depending on technological, doctrinal, ideological etc. influences. Generations of warfare will evolve because the war itself has undergone many *“qualitative changes”*. Generally speaking, optimistic analysts support the idea that a new generation of warfare will emerge whenever previously unnoticed issues are discovered: *“…generations will never end. They will continue to appear, one after another, ad infinitum, in all form of defence literature.[…] because enthusiasts will convince themselves that they have discovered a new generation of warfare every time they find some aspect of conflict they failed to notice earlier”* (Haug, Maaø, 2012, p. 49).

The emergence of a new generation of warfare bears the imprint of the previous generation, at least as a term of comparison and is shaped by the *“requirements of the conflict of the new type of society”* (Văduva, 2008, p. 37). In other words, analysed from this perspective, the concept of war *“is shaped according to the configuration of the world and evolves on the main coordinates on which the world actually evolves”* (Ibid, p. 20).

Although the generational approach is not an exhaustive one, it helps us to understand the complexity of the *“warfare”* phenomenon and, once we understand the particularities of each generation, we can also understand the coordinates on which the world evolves. In other words, knowing the directions of conflict development helps us to understand the present and to anticipate the future, within certain limits.

As Gheorghe Văduva mentioned, in a paper published in 2008, *“the knowledge of warfare, especially of the new warfare, i.e. the war or wars of the 4th generation, remains one of the great challenges of the present and the future”* (Ibid.).

This article aims at accomplishing the descriptive analysis of each generation of warfare, to identify the social, political, economic and technological changes that have shaped and customised each generation.

FROM THE FIRST GENERATION WARFARE TO THE THIRD GENERATION WARFARE. THE CONVENTIONAL NATURE OF WARFARE AS PERCEIVED FROM THE CURRENT PERSPECTIVE

The transformation of mercenary armies into national and professional armies was the basis for the emergence of modern nation-states. Therefore, the *"analysis of modern warfare should begin with the 1648 Peace of Westphalia, the settlement that ended the Thirty Years' War and established the state's monopoly on war"* (Lind, 2004, p. 12).

Since then, the nature of the warfare has changed, being characterised by: *"manpower"* – 1st Generation Warfare (1GW); *"Firepower"* – 2nd Generation Warfare (2GW); *"Manoeuvre"* – 3rd Generation Warfare (3GW).

To understand the Fourth Generation Warfare (4GW), it is important to be aware of the characteristics of previous generations of warfare. Therefore, the concept of 1GW appears with the advent of the modern state. Among its defining elements, we can itemise: the application of strict orders, culture based on obedience, compact fighting formations etc. The methods used are conventional in nature, emphasising the physical strength of the combatants. Also, the scope of the conventional refers to the existence of *"a military balance from a conceptual, organizational, technological and procedural point of view, a fact marked by violence, destructiveness and relatively long duration of the conflict"* (Mitulețu, 2018, p. 46).

The combat was between two states facing each other on a specific battlefield. The American counterinsurgency warfare specialist, Thomas Hammes, claims that the culmination of the First Generation warfare was the Napoleonic Wars at the beginning of the 19th century (Fridman, 2018, p. 20). At the same time, in the article *"Understanding Fourth Generation War"*, William Lind mentions that *"the main relevance of this generation of warfare springs from the fact that the battlefield of order created a military culture of order"*, as *"most things that distinguish military from civilians — uniforms, saluting, careful gradation of rank — were products of the First Generation and intended to reinforce the culture of order"* (2004, p. 12).

The Motto of the First Generation Warfare was *"close with and destroy"*, and the dominant feature was the strict organisation into line and column formations. *"The most prominent characteristic of first-generation warfare is 'line-and-column' tactics, whereby battles were formal and the battlefield was orderly"*. (Ibid., p. 20).

The transition from the First Generation Warfare to the Second was a lasting one, with gradual transformations taking place over several decades. Moreover, *"whereas the first generation of warfare was shaped by the 'line-and column' tactic that had required a mass deployment of manpower, the second generation warfare sought a solution in mass firepower, most of which was indirect artillery fire"* (Ibid., p. 21).

The regular armed forces, involved in the conflicts of the Second Generation, represented states, alliances or coalitions and the objectives were coordinated and subordinated by the political factor. At the same time, the patriotic impulse quickly changed the perspective of approaching conflicts: *"…the rise of nationalism, particularly in the period during and after the Napoleonic Wars, generated a patriotic impulse among the citizens of nation-states, ultimately bringing millions of men to the colours; this period of second-generation warfare would eventually culminate in the catastrophic losses incurred during the First World War"* (Hammes, 2004, pp. 18-20).

The most representative war in the 2GW category is the First World War, taking into account mainly the French experience, hence the French saying the artillery conquers, the infantry occupies, defining for the 2GW. The increase in firepower decreases the manpower and ideas begin to play an important role in the development of battle tactics. With the advent of weapons, the specific linear practice of the 1GW disappears, and the focus is on the detailed planning of artillery fire, with the synchronized execution of the manoeuvre. Also, the modernisation of warfare has led to an increase in striking power.

"Centrally controlled firepower was carefully synchronised (using detailed, specific plans and order) for infantry, tanks, and artillery in a 'conducted battle' where the commander was, in effect, the conductor of an orchestra. [Therefore] the focus was inward, on rules, processes, and procedure. Obedience was more important than initiative. In fact, an initiative was not wanted because it endangered synchronization. Discipline was top-down and imposed" (Fridman, p. 21). The Motto of the Second Generation Warfare was *"putting steel on target"* (Ibid. p. 21).

The Third Generation Warfare appears as a response to the increase in firepower on the battlefield. The Germans, based on their experience of the First World War and aware of the weak industrial background, decide to develop new tactics. Therefore, the 3GW corresponds to the German doctrine of World War II (Blitzkrieg), defined by trying to dominate the opponent by the manoeuvre. The 3GW is characterised by: non-linear tactics, the ability to engage fire, the execution of fire behind enemy positions, destruction of means of communication and transport, and high manoeuvrability.

"Similar to the first and second generations, the development of the third generation of warfare was not a sudden transformation but gradually evolved, with each military progressing at its own pace" (Hammes, 2004, pp. 23-30)

Based on manoeuvre rather than wear and tear confrontation, the 3GW was the first type of warfare to use non-linear tactics. In this type of conflict, the defence was done in-depth, the small units benefiting from great flexibility in decision making, to face the situations on the ground. The use of intelligent strategies could compensate for the technological disadvantage.

“A Third Generation Military focuses outwards, on the situation, the enemy, and the result then situation requires, not inward on process and method. Orders themselves specified the result to be achieved, but never the method. The initiative was more important than obedience” (Lind, p. 13). The Motto of the 3GW is “bypass and collapse” (Fridman, 2018, p. 22).

“Certainly, so-called traditional types of war, such as World War II, involve the use of every available network, by all principal parties. Even the strategic goals in that war went beyond defeating an opponent’s armed might to convincing political decision-makers that their goals were unachievable” (Haug et al. 2012, p. 52).

Upon a bird’s eye view, the three generations of warfare involved regular armed forces, actions aimed at repelling aggression or conquering territories, were destructive and violent, and battles and conflicts took place in the physical space, bearing a joint characteristic. Each generational change was marked by a large dispersal of the battlefield.

FOURTH GENERATION WARFARE, A COMPLEX AND LASTING CONFLICT OF UNCONVENTIONAL NATURE

At the end of the twentieth century, the confrontation reaches a new generation, the fourth. *“According to the advocates of 4GW, modern warfare is an evolved form of insurgency that employs all available networks—political, economic, social, and military – to convince an opponent’s decision-makers that their strategic goals are either unachievable or too costly”* (Echevarria, 2005, p. V).

There have been many contradictions on the subject of the 4GW. When Colonel T.X. Hammes defines the 4th generation war in his book *The Sling and the Stone as an Evolved Form of Insurgency* (Hammes, 2004, pp. 40), William Lind contradict Stone, claiming that he does not understand the 4GW theory very well. According to Lind, the 4GW is not at all a form of insurgency, but it rather refers to *who fights and what they fight for*. The emphasis is on the moral dimension[1] and not on the intellectual dimension of the conflict (Lesenciuc, 2016). However, Lind’s answer is also not clear, because there is no defining aspect regarding the development of the conflict, HOW? However, the war of the fourth generation concerns the decisions that the enemy makes at the political level. Through political, social and economic networks, as well as through military actions, 4GW actors seek to attack indirectly, aiming at weakening the enemy’s will to fight (remember the role played by the new paradigm of military thinking, defined by the *Strategy of the Indirect Approach* of BH Liddel Hart).

[1] In 2016, Adrian Lesenciuc coined the concept of *"moral asymmetry"*, in relation to this type of conflict.

Also, the 4GW marks the end of the era of states, and the protagonists of contemporary conflicts are state and non-state actors, the role of regular armies decreasing. The 4GW is characterised by the widespread use of technology, and the fact that many states are modernizing their armed forces can even be considered an *“optical illusion”*.

The actions of this form of conflict include society, culture, not just physical entities involved. In the 4GW *“the battlefield is the whole of the enemy’s society and the goal is to collapse the enemy internally, rather than physically destroying him”* (Lind et al, 1989, pp. 5, 8). Therefore, most military facilities (aerodromes, headquarters, etc.) are dispersed due to the vulnerability created by their concentration in one place.

The fundamental element of the 4GW is the belief that *“the superior political will on the part of insurgents can defeat a greater economic and military power”* (Sloan, 2008, p. 10). The 4GW-specific tactics and planning are very different from those of a conventional war. These are violent tactics (involving a wide range of actions, from complex low-intensity conflict to beheading videos, attacks on peacekeeping officers, or bombings on oil infrastructure, etc.), as well as non-violent tactics (use of the Internet and other media).

The distinction between peace and war, as well as between civilians and the military, may fade, or even disappear for good. The sphere of influence of the 4GW is reflected in several areas.

In the 4GW, opponents seek to manipulate the media to alter public opinion to the point where the use of psychological and information operations will exclude, in general, the engagement of armed forces into combat. Population support becomes the main target and information the most important operational weapon. Expansion in the media sphere represents a conceptual rupture in relation to classical conflicts.

“Fourth generations opponents are not invincible. They can be beaten, but only by coherent, patient actions that encompass all agencies of the government and elements of the private sector” (Hammes, p. 7).

FIFTH GENERATION WARFARE. ACTION DIRECTIONS OR PURE SPECULATIONS?

The evolutionary nature of the way wars were conducted led military theorists to question the emergence of the Fifth Generation Warfare. At the same time, despite the controversies regarding the clear delimitation of 4GW, some authors claim the existence of 5GW, even 6GW.

Even if the 5GW is less analysed, it is a confrontation involving irregular forces, without a centre of gravity, where state power is declining, while success varying inversely with the military power (Coerr, 2009, pp. 63). Even the use of violence may have some hidden logic because irrational and sudden destruction undermines the idea that nations are viable in the modern world. The 5GW is no longer a war in the true sense of the word. It is a unilateral war, in which it is not known who is *"fighting"*. The purpose of this type of war is to alter the relations of different natures, first of all, the economic relations. A conflict of the 5th generation carried out discreetly may manifest itself in such a way that the conflict cannot be explicitly understood within the limits of the definition of war. One can easily draw an analogy with the paradoxical explanation of the perfect robbery: *What does the perfect robbery look like? We will never know the answer because the bank will not know that it was robbed either*. Under these conditions, the simplest way to avoid war is the ability of states to produce subtle war, unidentifiable in these terms.

The 5GW could be the time when the future world powers will be able to adopt indirect means in their competition for power. China, Russia, India, the EU, as well as North Korea are also focusing their attention on this aspect of the 5th generation confrontation. The new era of warfare could be characterised by artificial intelligence and cyber warfare.

CONCLUSIONS

Any change, in any field, has effects on the understanding, planning and execution of military operations.

There are many theories about the generations of warfare, with some analysts even concerned with reinventing war so as for them to be one step ahead of the competition. Only critical thinking about the future, by imposing high standards in the military thinking, can avoid embracing *half-grounded theories*. Therefore, a rigorous comparative analysis of the generations of warfare could be a solution to understanding the conflict.

"Debating changes in warfare and how policies and doctrines should adapt to them can be beneficial, but only if we are willing to be rigorous" (Haug et al, p. 51).

Although some analysts argue that the generational approach is misleading, perhaps even artificial, portraying the types of confrontations in generational terms is just a way to analyse and understand how the phenomenon of war has evolved. We consider it beneficial to speculatively prospect the future, and in terms of the future of the military confrontation, this generational approach allows us to explore new perspectives and new possibilities.

BIBLIOGRAPHY:

1. Echevarria, A. (2005). *Fourth Generation War and Other Myths*. Carlisle, PA: Strategic Studies Institute.
2. Fridman, O. (2018). *Russian Hybrid Warfare, Resurgence and Politicisation*. Oxford University Press.
3. Hammes, T. (2004). *"4th-Generation Warfare: Our Enemies Play to Their Strengths"*. In *Armed Forces Journal*.
4. Hammes, T., *The Sling and the Stone: On War in the 21st Century.* St. Paul, MN: Zenith Press.
5. Haug, K.E., Maaø, O.J. (2012). *Conceptualizing Modern Warfare*. London: Hurst&Company.
6. Lesenciuc, A. (2016). *Războiul informational*. Brașov: Editura Academiei Forţelor Aeriene *"Henri Coandă"*.
7. Lind, W. (2004). *"Understanding Fourth Generation War"*. In *Military Review.*
8. Lind, W., Col. Nightengale, C. (SUA), Cpt. Schmitt, J.F. (USMC), Col. Sutton, J.W. (SUA), Lt.-Col. Wilson, G.I. (USMCR) (1989). *The Changing Face of War: Into the Fourth Generation*. In *Military Review*.
9. Mituleţu, I. (2018). *Schimbări de paradigmă în abordarea conflictului.* In *Revista Academiei de Ştiinţe ale Securităţii Naţionale*, no. 1.
10. Sloan, E. (2008). Military *Transformation and Modern Warfare: A Reference Handbook*. Praeger Security International. Westport, Connecticut, London.
11. Văduva, Gh. (2008). *Război şi cunoaştere*. Bucureşti: Editura Universităţii Naţionale de Apărare *"Carol I"*.

THE PERSPECTIVE OF WAR AND MODERN ARMED FIGHT

Second Lieutenant Olguța-Mihaela BODNAR

136th Engineer Battalion APULUM, Alba Iulia

This article addresses the current forms of modern warfare and armed fight based on Toffler's statement, "The world is constantly changing".

This change of the armed conflict is violent, explosive and very rapid, being like a reaction of the new to the old. The 21st century began in the spirit of this spontaneous reaction by producing structural changes in the concept of the armed fight, by adopting other forms of armed conflict than conventional ones, namely by asymmetric, irregular and hybrid conflicts in the last 10 years.

Military conflicts are like a chameleon, they change their colours to adapt to the new transformations of the security environment.

Keywords: modern armed fight; conventional; asymmetric conflict; irregular conflict; hybrid conflict;

INTRODUCTION

"The world is constantly changing" said Alvin Toffler in his book of the same name. Many of these changes are violent, explosive, being a reaction of the new to the old, of the old paradigms to the new, shaping real revolutions. Revolution in the military context refers to change, to progress, but it is not one-dimensional, like other revolutions. It is made on several levels, and if one of them is missing, it is no longer a revolution, but only an innovation, some progress.

The 21st century began precisely in the spirit of this new revolution in the military context, namely with asymmetric, irregular and hybrid conflicts, conflicts that give special importance to other means of fighting than the conventional ones, specific to armed fight.

The whole society has undergone changes in recent decades and the military institution has not been left out. The transformations it undergoes, in particular, the professionalisation of the military system and the ensuring of interoperability with the allied armed forces, in order to fulfil the objectives and missions entrusted, both at national level and in theatres of international operations, require special flexibility to adapt to the political-military global framework.

Against the background of the military transformations generated in the last part of the twentieth century and in the first part of the twenty-first century, some actors of the international environment have refined and, at the same time, diversified the methods and ways of waging war; thus, they have chosen to use different classical techniques of traditional warfare, combining them with irregular techniques belonging to the hybrid warfare.

This evolution of hybrid warfare has led some specialists to categorise it, through a very illustrative phrase, as a *"new, yet familiar"* threat.

Based on the above considerations, this paper can be a support in knowing the importance of the need for continuous adaptation to new technologies, new methods, techniques and tactics of combat, and understanding the current modern context of theatres of operations.

CONCEPTUAL DELIMITATIONS REGARDING THE EVOLUTION OF THE ARMED CONFLICT

In order to understand war and its evolution, it is essential to understand what the concept of *"war"* represents. The Merriam-Webster Dictionary defines war as *"military operations between enemies; an action lead by a political force (as nation) to weaken or destroy another"*. However, in military theory, the definition of war is often used as being the one given by Prussian strategist Carl von Clausewitz: *"war is a simple continuation of politics by other means"*.

Modern war, or rather war in general, is nothing but an expression of a reality beyond the conflicting limits of human society, namely an attempt to resolve a tense situation that could not be resolved diplomatically. War can be considered as a phenomenon, a given situation, which evolves at the same time with the human being, with society. The thresholds that the war has passed in its evolution are usually technological and doctrinal and these aspects refer to the term modern war.

Armed fight has always been the basic *"instrument"* of war. Even though military analysts believe that engaging in a traditional war is unlikely today, when NATO, the protective umbrella of the Alliance's member states, has in itself become a factor of stability and discouragement in the face of a possible trend of aggression against a member state, the study of armed conflict comes, however, from the possibilities of transforming risks and threats to state security into direct armed confrontation.

The diversity of armed confrontations and implicitly of armed fight appears as a result of direct or indirect interactions, of a complex of economic, social, political, technical-scientific, demographic, geospatial factors etc. As one of the main manifestations of war, the armed fight occupies a central place in it and materialises the concept of the use of the armed forces and their mode of action.

The armed fight can be considered *"as the mode of action of one of the instruments of politics – the armed force – in order to achieve the goals that politics could not achieve using its peaceful means"* (Ostropel, 2006, p. 4). It includes *"all actions carried out at the strategic, operational and tactical level by all categories of armed forces"* (Ibid). In a broader form, armed fight is the violent military confrontation between two militarily organised opposing forces with fighting power (intelligence, leadership, protection, manoeuvring, firing power), each aimed at the fulfilment of the proposed objectives. As a result of the impetuous development of the material means of the conflict, of the participation in the fight of some more and more diversified and complex forces, in its historical evolution the armed conflict resized its spheres of scope, changed its physiognomy and gradually acquired new underlying features *"modern warfare"* (Ibid).

The 21st century has brought major changes in the conduct of conventional military actions through factors with a special influence, specific to asymmetric, irregular and hybrid conflicts. One of the special changes in the evolution of the military phenomenon on the physiognomy of military actions is found as a reaction of the new to the old, a necessary reaction in the current conditions. The armed conflicts that have taken place in recent decades have shown that innovative thinking and technology are decisive factors in the design and modelling of confrontations.

Recent developments in the global security environment have rekindled debate in specialised media in the field of international relations and security studies on reconfiguring the international system and the emergence of revolutionary changes in the practice of modern warfare.

ARMED CONFLICT IN THE HYBRID WAR IN UKRAINE – CASE STUDY

The most recent modern confrontation is encountered in the conflict in Ukraine and is the most complex and complete form of hybrid warfare.

Hybrid warfare is characterised by military theorists as a social, complex, ambiguous and chaotic phenomenon, because it combines conventional and unconventional means to cause changes from the inside, by making the institutions and ideologies of the attacked state to lose their legitimacy and last but not least by wining the support of the local population in the conflict area to fulfil the objectives (Rațiu, 2016, p. 72).

American theorists say that hybrid warfare is *"a combination of symmetric and asymmetric war in which intervening forces conduct traditional military operations against enemy military forces and targets while they must simultaneously – and more decisively – attempt to achieve control of the combat zone's indigenous populations by securing and stabilizing them (stability operations)"* (Mc Cuen, 2008, pp. 107-108).

After the rapid annexation of Crimea and the outbreak of what initially appeared to be a similar conflict in eastern Ukraine, many perceived the Russian hybrid war as a new threat, a weapon that Russia could deploy anywhere and at any time.

In order to identify the premises for an irregular and hybrid conflict, it must be borne in mind that its initial, non-violent phases take place in full legality or somewhere at the limit of the law. The preparatory phase of the hybrid war does not differ so much from the conventional tools of Russian diplomacy, such as gathering information, establishing contacts with decision-makers, establishing media, supporting cultural projects and attracting non-governmental organisations. In fact, the preparations of a hybrid war are mostly build on these instruments that are long studied and experienced by the Moscow authorities, and which could be used in almost any circumstances (Bătinaș, 2017, p. 78).

The analysis of the whole spectrum of hybrid warfare is very complex. In the case of Ukraine, the hybrid war went on two fronts, namely the Crimea, where success was complete, and another, with partial success, in Eastern Ukraine, where the initial hybrid war was transformed into a conventional armed conflict, but limited (Ibid).

One of the peculiarities of the hybrid conflict in Ukraine, which is different from other conflicts studied, is that the subject of the hybrid threat, in this case Russia, is militarily stronger than the object of the threat.

The entire state has been *"infected"* with an extremely high level of corruption, including at the highest levels of state administration. Low government legitimacy was an additional factor that weakened Ukraine's resilience. This was noted during the Crimean crisis, when the new leadership in Kiev faced serious problems of legitimacy as well as functionality. Although the election of Poroshenko as president on 25 May 2014 contributed to the partial settlement of the issues of legitimacy, the difficulties related to functionality persisted. Russia and its local supporters have succeeded in taking advantage of the weak legitimacy of the new Kiev government in Crimea through the use of propaganda and the promotion of false news, significantly reducing the morale of Ukrainian forces stationed on the peninsula.

An important feature of the hybrid conflict in Ukraine is the massive presence of the Russian minority or Russian-speaking speakers. From a political perspective, the presence of ethnic Russians or Russian speakers in Ukraine could be a pretext for Russia that its actions were legitimate, because the purpose of the intervention was to protect the rights of ethnic Russians. From an operational perspective, it is much easier to find people dissatisfied with the central power among the Russian-speaking minority and to be recruited to be used against Ukraine.

The infiltration of special forces among the locals limited Ukraine's ability to use force against those who took part in illegal actions (Ibid).

In both Crimea and eastern Ukraine, the Russian press and the Ukrainian press under Russian influence succeeded in building an alternative reality in which they presented the fact that most ethnic Russians or Russian-speakers were in favour of secession from Ukraine, while in fact this did not correspond to reality (Ibid). The strong presence of Russian influence in the Ukrainian media allowed the attackers to generate and strengthen distrust in the central government, isolate the regions from any information coming from the capital, as well as mislead and misinform Ukrainians and the international community. The importance of a strong media and, in general, of the means specific to the information warfare, leads to the conclusion that these modern and cheap means are very effective in a modern war. Therefore, the impact that the media and the Internet have is directly proportional to the level of technological development of the actors involved in the hybrid war (Ibid, p. 80).

The implementation of the whole spectrum of hybrid warfare is not possible without providing adequate logistical support. Therefore, the military presence, even if undeclared, in the two areas of Ukraine was indispensable. This was facilitated by the common border between the two states, the presence of Russian military bases in the vicinity of the Russian-Ukrainian border and the non-existent or weak Ukrainian border authorities.

Russia's hybrid war in Ukraine aimed to annihilate Ukraine's ability to resist without using a large-scale military attack. This war was based on the combination of conventional and unconventional methods, with the engagement of the full spectrum of actions that include diplomatic, economic, political, social, informational and military means, all well synchronised so that the objectives are achieved.

CONCLUSIONS

In conclusion, while many countries have invested heavily in modernising conventional forces in recent years, the possibility of triggering a conventional warfare conflict has dropped significantly.

The latest military conflicts show the following: the future war will be multidimensional and will take place in all environments – on earth, at sea, in the cosmos, in the electromagnetic spectrum and in the intelligence sphere.

Intelligence warfare will be an increasingly important component of future wars and military conflicts, defying conventional methods of conducting military action and even many unconventional ones.

A concept that emerged and developed in the late twentieth and early twenty-first centuries, the hybrid warfare has changed the way traditional warfare is viewed.

One of the characteristics of modern armed conflict is that the barriers between the two stages of the war, the preparation and conduct of the war itself, have disappeared. At the same time, the preparation and conduct of war unite, complement each other, to form a continuous war, a much more dynamic war, waged more vertically than horizontally, a war of intelligence, and of hybrid actions.

The nature of complex missions in theatres of operations and conflict spaces is increasingly forcing military actors to be aware of the need for change, both technologically and professionally, as this must be done strategically so that reduce redundancy, improve efficiency and reduce potential damage.

On a different note, the modern, hybrid war is a surprise factor, an element that can shape the fate of a nation, can open new loopholes that develop military capabilities, help the evolution of military strategy, produce an increase in military professionalism due to the evolution of technology and its introduction to facilitate and digitise the battlefield.

In this sense, this paper presents the importance of finding a course of action that looks at both the conceptual and the conventional side, combining the elements to create a modern factor. At the same time, the importance of these evolutions and revolutions of modern conflicts will be highlighted, emphasising that the success of a mission is directly proportional to the symbiosis between conventional and unconventional military strategy, managing to balance and tip the balance towards success.

BIBLIOGRAPHY:

1. Bătinaș, V. (2017). *"Repere ale conflictului de tip hibrid în secolul XX şi începutul secolului XXI"*. (2017). Buletinul Universității Naționale de Apărare *"Carol I"*.
2. McCuen, J. (2008). *Hybrid Wars*. In *Military Review*.
3. Neag, M. (2010). *"Securitatea umană în conflictele și crizele internaționale"*. București: Editura Universității Naționale de Apărare *"Carol I"*.

4. Ostropel, V. (2006). *Considerații privind lupta armată modernă*, https://www.armyacademy.ro/buletin/articole/bul2ro_2006/a1.pdf, retrieved on 26 September 2020.
5. Rațiu, A. (2016). *"Amenințări și factori de risc la adresa securității globale"*. Sibiu: Editura Academiei Forțelor Terestre *"Nicolae Bălcescu"*.
6. Rațiu, A., Ostate, G. (2018). *"Studiu asupra specificului artei militare în conflictele de tip hibrid"*. Sibiu: Editura Academiei Forțelor Terestre *"Nicolae Bălcescu"*.
7. https://www.academia.edu/39070860/4GW_R%C4%82ZBOIUL_DE_A_PATRA_GENERA%C5%A2IE, retrieved on 26 September 2020.
8. https://www.armyacademy.ro/buletin/articole/bul2ro_2006/a1.pdf, retrieved on 26 September 2020.

DIMENSIONS OF HYBRID CONFLICT AND COORDINATES FOR COUNTERING ITS EFFECTS

Colonel Assoc. Prof. Aurelian RAȚIU, PhD

"Nicolae Bălcescu" Land Forces Academy, Sibiu

The fields of war have changed in time, which has caused transformations, both in the approach to confrontation and in the physiognomy and typology of actions. The military conflict has been characterised by irregularity: traditional and non-traditional actors acting directly or indirectly, with their own forces or through intermediaries (proxy forces), creating their own conventional or paramilitary military structures, and carrying out conventional actions concurrently with terrorist activities specific to insurgency or organised crime.

The solutions for countering the hybrid conflict must be understood in terms of summing up the known (conventional) and the less known characteristics of the conflict, as well as of developing new, unexpected, surprising (irregular) ones, determined by the evolution in the operational field.

Keywords: hybrid conflict; operational environment; hybrid threats; combating the effects of hybrid conflicts; area of responsibility;

INTRODUCTION

Given the interdependence within the relations between states regarding the sectors of economics, security, proliferation of risks and irregular threats (terrorist attacks, attacks with biological agents, with vectors carrying CBRN substances, informational aggressions, cyber or geophysical attacks, organised crime, illegal migration) and of the globalisation of the field of confrontation between the multitude of actors, it becomes obvious that the *hybrid war/conflict*, in the current sense, can be considered an actual, dynamic and very complex concept.

The issue is relevant from the perspective of both the effects of hybrid threats that spread in all confrontation environments and the permanent adaptation of military structures and the development of complementary capabilities in order to be able to meet these challenges in a pertinent and effective manner.

HYBRID OPERATIONAL ENVIRONMENT AND HYBRID CONFLICT DIMENSIONS

In the light of the existence of threats, *aggressions* and *hybrid operations*, the following question arises: where are these carried out? Therefore, the environment in which they take place is characterised by a wide range of components: the actors, the physical space (land, air, naval, cosmic) of the actions, information, technology, cultural environment, risk factors, threats, etc.; basically, a mix of elements whose combination leads to something complex and new, to a *hybrid environment*.

The operational environment in the current context can be understood as a range of conditions, circumstances and actions created by the multitude of actors that interact in a certain area pursuing their own interests and that influence the decisions regarding the employment of the military and non-military capabilities at their disposal, in order to achieve the expected goals. The hybrid operational environment, in another perspective, represents *"the framework for the manifestation of hybrid threats, and it implies the complex and combined configuration of the chessboard of actors, means, actions that converge in a concentrated manner and most often in secret, towards fulfilling the pursued goals"* (Ganea, 2016, p. 65).

In general, the most important constituents of the hybrid operational environment could be the following: *Physical environment/domain (land, air,* *sea); Actors that produce threats and dangers; Civilian/local population; Agencies and organisations; Independent actors; Unknown actors; Information and cyber environment*.

Physical Domain/Environment (land, air, sea)

The physical domain is the land, air, sea and *space environment* in which/on which the forces/capabilities of the parties will confront each other in order to achieve their interests/objectives. Thus, this scientific approach refers to some less studied aspects of the dimensions of the hybrid conflict, such as: *aerial* and *maritime*, in comparison with the others, terrestrial and informational ones.

The land domain is the terrestrial/dry geographical environment (the surface of the lithosphere) including all its natural elements, as well as those created by the human hand, which, one way or another, influence the organisation, preparation and conduct of conventional or unconventional actions. The forces will act in a variety of areas, both in the classic ones: planes, hills, plateaus or mountain-forested land, and in other regions, such as the Arctic, the coastal (seaside), jungle, desert or urban areas. Campaigns often involve a *combination of such environments*.

The physical domain for *the maritime component* (sea and river forces) is represented by *oceans, seas, rivers, sunken lands* and *inland waterways*. The maritime environment – the surface of the oceans, seas, rivers and their depth (the underwater space) is the place where the actions of the naval component take place and represents two thirds of the planet's surface. The maritime environment allows forces to have access to the coast, to have mobility, projection and logistic autonomy. The maritime activities are influenced by the meteorological, oceanographic and geographical conditions of the marine environment: the size of the waves, the force of the wind, the speed of the currents, the temperature of the air and the water, the transparency of the water, the tides, the salinity and the density of the water, the characteristics of the bottom of the waters (sea, canals and rivers) – factors that also influence the ability of ships to navigate and use the weapon systems.

The air force, which operates mainly in the air and space environment, essentially changed the conflict paradigm. *The air domain* is *"that continuous environment that surrounds the entire planet, being delimited only by the land surface and the sea surface. This feature facilitates certain differentiated advantages compared to the terrestrial, maritime and underwater environment, generated by a certain freedom of action, constrained only by the performance of the aircraft at the geophysical borders and the abilities of the crews"* (Roman, 2017, p. 20). The emergence of hybrid threats in the airspace complicated the intervention of the elements of air force in the conflict equation, through the prism of the air force capabilities and their role in relation to a hybrid adversary.

Actors Producing Hybrid Threats

Threats can occur in different forms, coming from groups such as (Rațiu, 2020, p. 46):

- conventional military forces, easily identifiable on the basis of uniform and the weapons *"worn in plain sight"*, acting conventionally/traditionally;
- unconventional/irregular forces, difficult to identify, acting through a combination of violence and subversion: proxy forces, terrorist networks, guerrilla groups, organised crime cartels, ideological groups capable of building paramilitary structures or transnational terrorist networks, hackers or groups of hackers, organizations specialised in laundering and recycling dirty money, mafia associations, pressure and destabilisation groups, etc.

In some cases, opposing forces can produce *hybrid risks* or *threats*. In such cases, a grouping may combine the conventional forces/actions and the unconventional forces/actions in a complementary manner. In other cases, a single force can in itself adopt a combination of actions with conventional and unconventional characteristics.

A) *On the ground*, some potential adversaries may use advanced weapon systems in irregular/guerrilla tactics or change irregular and conventional tactics, depending on the situation. Generally, the proxy, guerrilla military forces use conventional weapons against security structures, but in different tactics, of hybrid type, such as: the placement of improvised explosive devices, hastily prepared attacks and ambushes, indirect fires with the help of more or less advanced, perhaps even improvised, systems, acts of terrorism (suicide/kamikaze attacks, assassinations, kidnappings and false imprisonments).

B) *Naval* military confrontations have a predominantly offensive character and imply continuous manoeuvrability. Most of the time, the actions of conventional and unconventional naval forces will start at sea and end on land. To do this, it is operated both with large battleships and with small, fast means, easy to manoeuvre, with good protection of the embarked forces, and also with considerable striking power. International terrorism acts not only *on land but also on the sea* and it represents a real and complex threat. Preventing terrorist attacks on or from the sea, as well as countering the illegal crossing of maritime borders by terrorists, became a major concern for the states with access to seas and oceans. Terrorism and associated actions had the effect of increasing the number of *maritime piracy* acts. Moreover, the identification of the common interests of the *terrorists* and *pirates* led to the coalition and even the unification of the groups, to the extension of the areas of action and also to qualitative changes in techniques of action and in the used arsenal.

C) *Airspace* capabilities respond to a wide range of threats, threats that are used during both conventional and unconventional operations: multi-role fighter jets, attack helicopters, unmanned aerial vehicles, anti-radiolocation missiles, ballistic missiles, tactical missiles, ISR – Intelligence, Surveillance, Reconnaissance capabilities.

The most relevant threats remain the conventional, traditional ones, consisting of fighter jets and helicopters. However, it is estimated that the use of unmanned aerial vehicles has recently gained ground. In addition to conventional threats, state and non-state actors make extensive use of other hybrid air threats, in particular civil aircraft (use of passenger planes as a weapon during the September 11, 2001 attacks in the United States) – *RENEGATE threats*, small unmanned aerial vehicles (drones) or the use of anti-aircraft missile systems to shoot down civilian aircraft (as in Ukraine and Iran).

Civilian/Local Population

Most actions and campaigns are carried out among or affecting the civilian population and the military and security structures will have permanent contact with the local population. This requires leaders/commanders at all levels to consider, from the time of planning, the effects that security operations will have on civilians, local communities and infrastructure. Approaches in this regard may vary:

- in *conventional confrontations*, the aim is to avoid the production of victims among civilians by evacuating and/or relocating them, arranging refugee camps, etc., and, also, to avoid damaging civilian infrastructure;
- in *hybrid conflicts*, operations focus on protecting the civilian population against attacks and abuses from opposing groups, on combating the effects of their psychological actions, and on support actions (rebuilding/building infrastructure, offering medical and educational services, etc.) so that government and the international coalition/alliance forces gain authority and legitimacy (thus, the neutral civilian population supports the government component).

The civilian population and society as a whole are the centre of gravity in the hybrid war. The attractiveness regarding the use of the population/society derives from *"the large dimensions, the structural heterogeneity, the ease of producing the desired effects, the existence of possible fault lines between ethnic groups (breaches in the homogeneous character), the involvement of segments of population extremely permissive to certain messages, offering the possibility of manipulation"* (Mihalcea, 2018, p. 18). All the listed elements can represent vulnerabilities and can be speculated by the conflicting entities.

Agencies and Organisations

Relevant institutions/agencies and organisations can be represented by local and international government departments/institutions, host nation security forces, coalition military forces, non-governmental organisations (NGOs), private security organisations and even independent businessmen.

In the current operational environment, national and coalition military/security forces, following the model of the hybrid approach, are no longer at the forefront, as in war, but have a well-defined role by getting involved in supporting the actions of other governmental and non-governmental agencies and organisations to reach various objectives: political, economic, social, military, cultural, etc.). Moreover, in order to generate the necessary conditions for government institutions and civilian bodies to achieve lasting effects on the political, economic, social, etc. level, the military instrument is directly involved in conducting actions extremely necessary to create a climate of security and stability.

Unknown and Independent Actors

Some actors in the operational environment will be considered *unknown* in terms of the support (given or not) of the campaign/forces pursuing security. Indigenous actors will support the campaign if they believe that the final goals and objectives, as well as the methods/means of achieving them, are legitimate or support their own interests. Their perception of legitimacy will depend on their culture and social expectations. Thus, the perceptions and interests of these actors need to be understood in order to act in their support and to protect them for the benefit of the campaign. Some actors will act completely independently *(independent actors)* from legitimate government forces, even if their ultimate goals are the same as those of the campaign. Such groups will avoid interaction with military forces, pursuing their own goals. The decision-makers need to be aware of the presence of such organisations in the area of responsibility and especially of the effects of their actions, and how they can affect the fulfilment of the assigned objectives (NATO Chiefs of Staff, 2016, pp. 1-5).

Information and Cyber Environment

The information environment represents the cognitive, virtual and physical domain for all the actions and processes that involve gathering, processing and using information. The information environment is composed of *"individuals, organizations and systems that collect, process, disseminate or act on information"* (US Department of Defense, 2016, p. 2).

The information is the link between the physical environment and the other areas that the actors involved use the integrating element of all the actions taken to reach the set objectives.

The decision, in any field, but especially in the field of conflict management, requires timely, accurate and rigorous information, and prediction regarding the need for information plays a particularly important role in the context of ambiguous situations specific to hybrid confrontations.

Currently, the whole company is connected in a *"network"* (Internet network, GSM communication systems, social networks, etc.), which allows both state and non-state actors to use the techniques and means specific to the information environment to reach their goals. They use a variety of means to exploit, disrupt or disable decision-making systems, to misinform and promote propaganda products, to strengthen internal resistance, to recruit supporters, to solicit funding and to promote the legitimacy of their actions, simultaneously with discrediting the actions of other actors, these actions and activities taking place in the information environment.

A significant component of the information environment is the *cyber space*, which overlaps the physical and information dimensions. It is essential that the analysis of the information environment also include actions in the cyber space and the identification of key individuals and groups influencing decisions and the native civilian population through *cyber space*. The *cyber space* represents *the virtual environment, generated by cyber infrastructures, including the processed, stored or transmitted information content, as well as the actions carried out by the users in it* (Guvernului României, 2013, p. 7).

The power offered by the information technology and the means within the cyber space is part of the hybrid war as a strategy for state or non-state actors to achieve their objectives.

The maximum benefit of any form of attack realized in the cyber space increases when this form is integrated with the other methods and means of attack, becoming a complementary element and leading to the *hybridisation* of the confrontation. The use of hybrid elements provided by the cyber domain (cyber attacks, propaganda through the virtual environment, social networks, etc.) can be a factor of force multiplication.

IMPERATIVES IN COMBATING THE EFFECTS OF HYBRID CONFLICTS

For a better understanding of the operational context of hybrid confrontations, of the nature of these types of threats, it is necessary to identify the imperatives and then the directions of action to limit or eliminate the specific risks.

The imperatives in the hybrid confrontations are represented by the context of the changes in the operational environment and by the available means used in the combat strategies.

The cognitive imperative. It refers to the cognitive-psychological component of hybrid warfare and implies a good understanding of the operational environment in the area of responsibility, so as to identify the best methods and tools through which a certain perception of the adversary is generated, so that the opponent, involuntarily, decide and act to his disadvantage. This idea is included in the concept of reflexive control, a concept from the Eastern region, which involves *"the action of providing an adversary with specially prepared information that will lead him to a voluntary decision that benefits the initiator of the action"* (Georgescu, 2016, p.79).

This nonlinear approach is, in fact, an atypical way of thinking, which creates the conditions for implementing power/influence in areas of interest, the simultaneous use of an extremely varied range of non-military methods and means aiming at concealing real geopolitical, military, economic etc. intentions and influencing the adoption of predictable decisions by competitors. The main purpose of these actions is to create a direct, rapid and significant impact on the efficiency of the military and non-military measures that the adversary takes.

In this regard, the operational approach must be able to ensure the most effective counteracting of the cognitive aspect of hybrid threats, through articulated actions that can be carried out at all levels, by employing the most appropriate capabilities. These actions must be carried out in such a way as to have the effect of effectively counteracting the threats and creating the necessary conditions for further action.

The imperative of a comprehensive approach. In the context of opponents using hybrid threats, the imperative of the comprehensive approach refers to the creation of opportunities for tactical, punctual/domain-based operations, and also actions aimed at generating strategic and chain effects with implications in many areas. It is about combining efforts to understand the phenomenon of hybrid warfare and to develop mechanisms for early identification of the threat and responding effectively to hybrid aggression. Fighting hybrid threats is a very complex activity, and the measures taken to limit their effects go beyond the scope and responsibility of a single actor/institution, involving a *comprehensive approach* – combining/integrating in time and space the efforts of all power instruments, actors/parties involved, both internally and especially internationally.

Pattern imperative – involves avoiding organisation, planning and linear, uniform development of actions/measures in time and space. Based on a good knowledge of the complexity of the operational environment, this aspect is relevant for avoiding surprise, by means of thinking, concepts and measures that circumvent the doctrinal approach to operations. While the military regulations require establishing clear and precise procedures, the new operational vision requires from the leader a much more in-depth analysis of the situation and the factors, an approach different from the dogmatic, traditional one being imperative.

The analysis of these imperatives reveals an intrinsic connection between the cognitive field of understanding the complex adaptive systems in the hybrid conflict and the physical field, between the violent and non-violent, military and non-military component and the efforts of the power elements at all levels.

These imperatives are considered to be essential because their understanding facilitates taking the necessary measures for the management of hybrid conflicts at decision level.

CONCLUSIONS

The complexity of the hybrid conflict includes violent and non-violent, politico-diplomatic, informational-propagandistic, commercial-economic with corruption elements, research-diversionist partisanship, energy and critical infrastructure, cyber, CBRN etc. military methods and means.

Thus, the effects of hybrid conflicts are propagated in all the environments in which the conflict takes place, whether we refer to the land, air, maritime, information and cosmic domain, or to other areas of social life: political, economic, diplomatic, cyber, social, cultural, religious etc.

Any response to hybrid threats will require a comprehensive/integrated approach by employing a wide array of military, non-military, governmental and nongovernmental instruments.

Integrated actions (interagency, inter-institutional), placed on a higher level, will not only mean the cooperation or joining of governmental instruments, but also their merger/integration, involving international or non-governmental organisations as well.

BIBLIOGRAPHY:

1. Ganea, I. (2016). *Noul mediu de securitate şi consecinţele sale. Războiul hibrid ca fenomen actual*. Bucureşti: Revista Oștirii Române, no. 1.
2. Georgescu, D. (2016). *Războiul hibrid – cea mai complexă formă de aplicare a artei operative*. Bucureşti: Buletinul Universității Naționale de Apărare *"Carol I"*, no. 2.
3. Mihalcea, V.C. (2018). *Fundamente şi ţinte ale războiului hibrid în acţiunile beligenei contemporane*. Bucureşti: *Infosfera* Review, no. 1.
4. Rațiu, A. (2020). *Conflictul hibrid. Forme de manifestare și modalități de gestionare.* Sibiu: Editura Academiei Forţelor Terestre *"Nicolae Bălcescu"*.
5. Roman, D. (2017). *Riposta antiaeriană a Forţelor Terestre din perspectiva modelelor conceptuale de lucru colaborativ*. Bucureşti: Editura Universităţii Naţionale de Apărare *"Carol I"*.
6. Chiefs of Staff (2016). *AJP-3.2.-Allied Joint Doctrine for Land Operations*, Brussels: NATO Standardization Office.
7. Guvernul României. (2013). *Strategia de securitate cibernetică a României. Monitorul oficial*, no. 296 of 23 May 2013, https://cert.ro/vezi/document/strategia-de-securitate-cibernetica, retrieved on 29 March 2020.
8. US Department of Defense. (2016). *Strategy for Operations in the Information Environment*. Virginia: Department of Defense, SUA, https://dod.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf, retrieved on 19 March 2020.

CYBERSPACE IN THE OPERATIONS PLANNING PROCESS

Lieutenant Colonel Nicolae-Sorin MACOVEI

"Nicolae Bălcescu" Land Forces Academy, Sibiu

Ensuring cyber security has become increasingly important and culminated in the recognition of cyberspace as an operational environment, along with land, water, air and space.

Operations in the cyber environment must be planned, integrated and synchronised with operations in other operational environments. The armed forces carry out cyberspace operations and support activities in this field as part of the joint operation.

In the modern war, the superiority in the cyber environment ensures a decisive advantage to the commanders from all echelons. This is achieved through a human, technological and procedural combination. The military is accustomed to seeing the effect of their actions on the battlefield, in a physical environment. However, cyber operations take place in a virtual environment, and their effects are sometimes difficult to identify.

Keywords: cyberspace; cyber operations; planning process; tactical level; operational environment;

INTRODUCTION

Technological progress is what has led to major changes in the physiognomy of military conflicts and continues to be the main factor of change in terms of both the spectrum of threats and the development of new weapon systems.

Technological progress usually leads to major changes as far as the action and concepts are concerned, and the laws of the armed fight, which refer to the dependence of organisational structures, forms and procedures, confirm that technological progress produces major changes in the theory regarding the armed fight in almost all areas. Moreover, technological progress has led to the emergence of new operational environments, and cyberspace is a concrete example in this respect. Thus, in this space without physical limits, it is necessary to adopt new forms and procedures of action under the new technological and tactical capabilities. These capabilities determine organisational changes by creating more flexible structures with increased mobility, as well as the emergence of new military structures and specialities.

Technological progress for both computer system components and hardware devices used in communications networks has evolved exponentially lately (*Moore's Law and the Future of Mathematics*). This progress brings great benefits for commanders and staff because functional applications are made available, operational or tactical situations can be viewed in near real-time and the exchange of information that takes place in a very short time helps to optimise decision-making. However, given these benefits, through the technology used and their configuration, modern communication and IT systems are as vulnerable as any other computer system. The more computerised a command and control system (C2) is, the more vulnerable it is, and the security of communication and IT systems is a continuous and major concern for specialised personnel.

CYBERSPACE – FROM CONCEPT TO OPERATIONAL ENVIRONMENT

Over time, ensuring cyber security has become increasingly important at both NATO and EU level. The 2002 Prague Summit was the first time the Alliance's cyber security was addressed at a strategic level among allied states, and the need to protect the computer systems used was emphasised. At the Riga Summit in 2006, the Alliance's first cyber security strategy was issued, a strategy materialised in *"Policy* *on Cyber Defence"*. After its recognition, at the Warsaw Summit in 2016, as an operational environment, along with land, air and water, cyberspace has been given due importance. The cyber defence has become part of NATO's basic collective defence requirements. The Alliance must be prepared to defend its networks and operations against increasingly sophisticated and numerous cyber threats and attacks. Since 2016, the Alliance has made the field of cyber defence a top priority.

In 2018, at the Brussels Summit, the Alliance agreed to set up a Cyber Operations Command as part of NATO's Command Structure, designed to become fully operational in 2023 (Emmott, 2018). The following year, in February 2019, the Alliance endorsed a NATO guide that set out a set of tools to further strengthen NATO's ability to respond to malicious cyber activities.

In Romania, 2013 was the year when *Romania's Cyber Security Strategy and the National Action Plan on the Implementation of the National Cyber Security System* appeared. Through it, *"Romania aims to ensure the state of normality in the cyberspace by reducing risks and capitalising on opportunities, by improving knowledge, capabilities and decision-making mechanisms"* (Decision no. 271/2013, p. 11).

In the *Security Strategy*, four directions of action have been established to achieve this goal:

- setting the conceptual, organisational and action framework necessary to ensure cyber security;
- developing national risk management capacities in the field of cyber security and response to cyber incidents based on a national programme;
- promoting and enhancing the cyber security culture;
- developing international cooperation in the field of cyber security (Ibid, p. 11).

The United States Armed Forces, as well as other NATO armed forces, have updated their doctrines and textbooks to the new concept of cyberspace. Thus, in June 2018, the *Joint Doctrine for Cyber Operations (Joint Publication 3-12)* was republished which supports the planning, execution and evaluation of cyber operations.

The tactics and procedures for coordinating and integrating cyberspace and electronic warfare operations in support of land and joint operations were published in Field Manual (2017) – *Cyberspace and electronic warfare operations*. In this manual, in addition to the fundamentals of cyber operations, the terms and definitions specific to the field, as well the role, resources of commanders and the way to evaluate operations are presented.

In *Army Doctrine Publication* (2019), cyberspace is integrated as an information environment, along with the other components of the combat space (land, air, sea, space).

The Romanian Armed Forces have tailored to meet NATO trends. On 1 December 2018, the Cyber Defence Command was established, as the authority of the Ministry of National Defence in charge of cyber security, cyber defence and information technology, and in August 2020 the *"Doctrine of Cyberspace Operations"* was drafted.

CYBERSPACE IN THE CONDUCT OF OPERATIONS

The operations environment is characterised by complexity and dynamism and can be extended to all operational environments, thus becoming a multidimensional one. These characteristics are the result of the interactions, relationships, conditions, circumstances and influences of the different variables existing in the battlefield.

Cyberspace operations need to be planned, integrated and synchronised with joint operations. The armed forces carry out cyberspace operations and support activities in this field, as part of the joint operation. In the modern war, the superiority in cyberspace ensures a decisive advantage to the commanders from all echelons.

In order to create the specific effects of this operational environment, cyberspace missions require the engagement of various types of actions. These consist of defence actions, attack actions, intelligence gathering, surveillance and reconnaissance (ISR), Operational Preparation of the Environment (OPE) and security actions, all related to cyberspace (Intelligence, Surveillance, and Reconnaissance Design for Great Power Competition, 2020). In order to plan, carry out and evaluate these actions, it is important to understand the differences between them and the purpose of each.

The military men are accustomed with seeing the effect of their actions on the battlefield, in a physical environment. However, cyberspace operations take place in a virtual environment, and the effects are sometimes difficult to identify by non-specialised staff or are sometimes identified too late.

How an opponent can attack the hardware and software infrastructure, having as result the destabilisation of the Command and Control System, is represented by the cyber attacks that take place of course in cyberspace. The *cyber attack* is defined as a *"hostile action carried out in cyberspace that could affect cyber security"* (Decision no. 271, p. 7), several operations being carried out to reduce the attack area.

Cyber defence actions are those *"actions carried out in cyberspace to protect, monitor, analyse, detect, counter aggression and ensure timely response against threats to cyber infrastructures specific to the national defence"* (Ibid, p. 7). These types of actions are critical to ensuring the functioning of communications and IT systems and are usually taken by specialists who plan, organise and operate communications and IT systems and networks.

Information gathering, surveillance and reconnaissance (SRI) actions are carried out in cyberspace to gather the information needed to support future cyber attacks or defences. These actions support the planning and execution of current and future cyberspace operations *(figure 1)*.

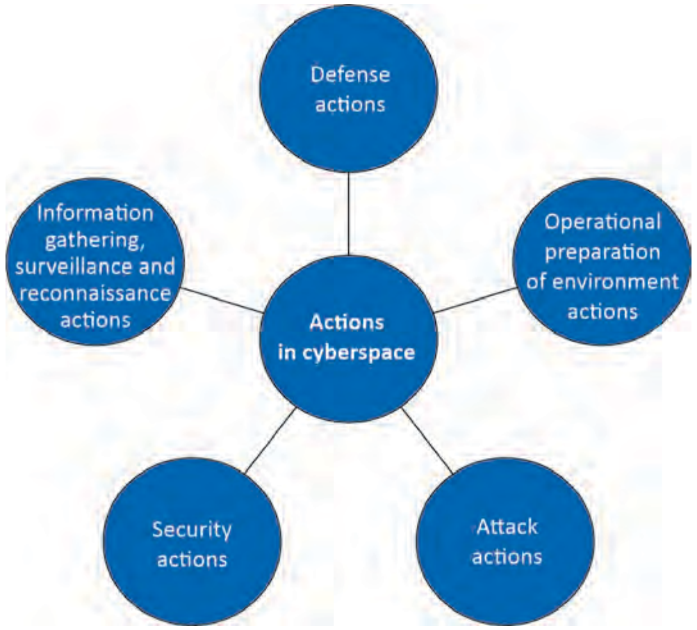

Defense actions
Information gathering, surveillance and reconnaissance actions
Operational preparation of environment actions
Actions in cyberspace
Security actions
Attack actions

Figure 1: Types of cyberspace actions (FM 3-12, p. 1-19)

Operational preparation of environment (OPE) measures are activities carried out for planning and preparing potential military operations, but not related to the information environment (Ibid.). These include identifying data and information, system/network configurations, or the physical structure that connects a network or system (applications used, ports, assigning network addresses, or other identifiers) to determine system vulnerabilities. We can add here actions taken to ensure access and/or control over the system, network or data during potential hostilities.

Security actions aim to achieve the *"state of normality resulting from the application of a set of proactive and reactive measures that ensure the confidentiality, integrity, availability, authenticity and non-repudiation of information saved or in transit, public or private resources and services, from cyberspace. Proactive and reactive measures may include security policies, concepts, standards and guidelines, risk management, training and awareness-raising activities, implementation of technical solutions for cyber infrastructure protection, identity management, consequence management"* (Decision no. 271, p. 7).

Cyber security is achieved through technical, procedural and human measures. The human factor is the one who combines all security measures. Thus, to ensure cyber security, the challenges and threats in the new (cyber) operational environment must be known by all users/operators of information systems. There is a need to create, develop and train a culture of cyber security. Most computer-system users are unaware of this phenomenon and identify the need to develop a cyber security culture among them.

Computer networks of own and enemy forces, communication systems, computers, cell phone systems, social networking sites and technical infrastructures are some of the main components of cyberspace.

Although cyberspace coexists with other operational environments, it is a separate environment. It penetrates land, air, sea and space operational environments through communications and computer networks interconnected through various transmission media. Freedom of manoeuvre in cyberspace allows mission control and freedom of manoeuvre in other areas. Each physical operational environment has its cyber environment, and taken together, they form the combined cyber environment.

CYBER SPACE IN THE PROCESS OF PLANNING OPERATIONS AT A TACTICAL LEVEL

Given the importance cyberspace has reached in conducting military operations, it should play a similar role in the planning of operations. Operations' planning in cyberspace is an integral part of the operations planning process, intending to develop the specific annexe to OPORD/OPLAN.

Commanders at all levels must be aware of the importance of cyberspace in achieving the objectives and mission received. A well-performed enemy cyber attack can have the same effect as an artillery fire on the command point, respectively its decommissioning.

Cyberspace operations can be very complex and, to carry out an efficient planning process, it is recommended that four levels of planning for these operations are considered: technical, tactical, operational and strategic. Therefore, compared to the process of planning operations in a traditional operational environment, where it is carried out on three levels, in the case of planning cyber operations, the technical level must be the starting point. Proper incorporation of technical aspects is of critical importance in the conduct of effective cyberspace planning *(figure 2)*.

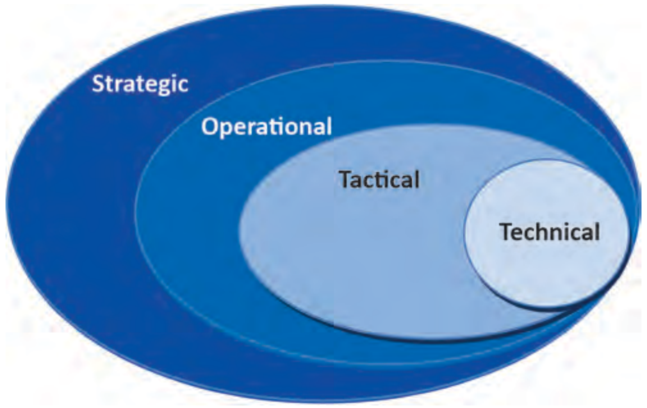


Figure no. 2: Planning levels (Barber et. al., 2015, p. 3)

Commanders do not as intuitively understand the technical details associated with cyberspace operations and planners as they do with the capabilities and limitations of combat technique (tanks, ships, or aircraft). The complex and dynamic nature of cyberspace, as well as its technical characteristics, often leads to the analysis and planning of operations beyond those planning practices and procedures found in traditional doctrine.

Cyberspace operations planning takes place simultaneously with the operation planning process, following its stages and phases. The products resulting from the planning are usually those provided in the Operations Planning Manual.

Given that there are still no specialised structures for cyberspace operations[1] at the tactical level, the planning tasks are distributed to the staff of the unit's staff. Staff members responsible for the planning and integration of cyber operations participate in the activities of the decision-making process.

[1] The new NATO capability targets stipulate the establishment of regulatory and command elements at the strategic and operational level, respectively tactical level execution structures, equipped and properly trained, able to execute specific actions in Cyber Security.

An important role in the operations planning process is played by the information structure, which will carry out the activity of information preparation of the battlefield, including the cyberspace. It is a challenge for the intelligence structure because the employees involved in this activity must be trained and know the peculiarities of the cyberspace. To perform this task as efficiently as possible, it is recommended that the intelligence structure cooperates closely with the planning structure of the IT and communication networks, namely the communications and IT structure.

A complex analysis provides the people involved with the relevant information to understand, visualise and describe the operational environment, and the decision made may be relevant.

Cyberspace, as part of the operational environment, must be analysed in the first phase from the perspective of the information environment. The information environment is characterised by the physical, information and cognitive dimensions.

The physical dimension of the cyber environment is represented by the physical elements of the network that include communication networks, computer systems and network infrastructures. The physical dimension provides access and control of information and data by users, represented by individuals or groups.

The information dimension is represented by the information that can be found in one of the two states: in transit or saved on disk. This dimension is directly connected to cyberspace due to the volume of information saved or in transit; it ensures the collection, processing, storage, dissemination and display of text, images or data. The informational dimension ensures the connection between the physical and the cognitive dimension.

The cognitive dimension includes the knowledge of those who transmit, receive, respond to or act on information. The cognitive dimension in cyberspace is represented by individuals, groups or organisations. Cyberspace connects the data and ideas of those who send, receive, respond to, act on, or add new information (FM 3-12, p. 1-13).

At the same time, the cyberspace is described as a sum of 3 layers: the physical layer, the logical layer and the *"cyber-persona"* layer (FM 3-12, Ibid.), layers that allow the understanding of the context and the creation of operational opportunities.

The physical layer of cyberspace refers to that geographical component as part of the physical dimension. The geographical component, in the present situation, represents the location of the network elements in one of the terrestrial, aerial, maritime or cosmic operational environments. The physical layer consists of hardware components, system applications and infrastructures (wire, wireless, cable links, electromagnetic, satellite or optical waves) that make up the network and the existing physical connections (wires, cables, radio frequencies, switches, servers and computers).

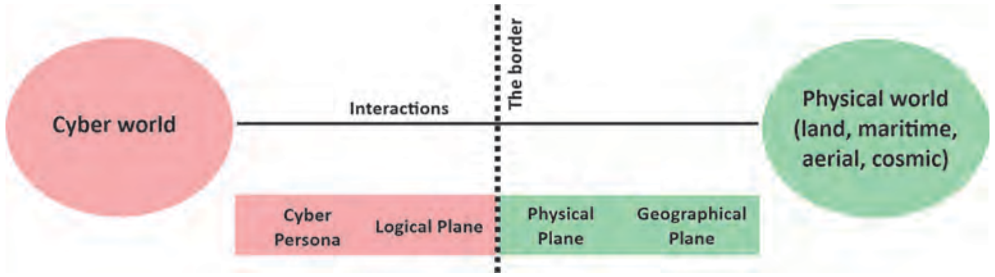


Figure 3: Planes of cyberspace (Azmi, 2019, p. 25)

The logical plane consists of the interconnection of the components of the physical network in an abstracted way. For example, network nodes in the physical plane can logically connect to form entities in cyberspace, but physically they do not depend on a particular node, path, or individual.

The cyber-persona plane is a digital representation of individual identity or entity in cyberspace. This plane is represented by users or consumers of network services.

It can be said that cyberspace is represented by communication networks and computers interconnected by the logical plane, which allow information to be accessible from any point, using the physical plane consisting of wired or wireless connections with high data transfer speeds, which is accessed by people using the cyber-persona plane.

In the intelligence analysis of the cyberspace, the analysis of these dimensions and planes provides an overview, but to have a complete image, its characteristics must be taken into account.

To identify the characteristics of cyberspace, we must start from the definition – an extensive and complex network, consisting of network nodes that are found in each operational area, connected by different transmission media. Therefore, the first feature of cyberspace is the *network feature*. The core of these networks is the technological infrastructures consisting of several distinct enclaves connected in a single logical network that allows the transport of data. The identification of these infrastructures and operations is done by analysing the planes of cyberspace, the dimensions of the information environment, the variables of the operational environment and other technical aspects specific to wired and wireless communications and IT networks (FM 3-12, p.1-15).

Because cyberspace provides interaction between individuals, groups, organisations, and states, another feature of cyberspace is the social feature. Computer systems and computer networks enabled the possibility of quickly creating, storing, processing, manipulating and transporting data and information for a small or very wide audience. Text messaging, e-mail, social networking sites and other forms of interpersonal communication are possible due to cyberspace.

Technological progress increases the complexity of the hardware and software components and devices of the communications and computing system, and as cyberspace is dependent on these components, it can be said that technological progress directly influences cyberspace. In other words, another feature of cyberspace is the *technological feature*. Moreover, it is a requirement that the personnel operating these pieces of equipment be one with intensified technical skills.

Interdependence and interrelationship are also specific to cyberspace, as operations in the other four operational environments are dependent on cyberspace. Besides, there is interdependence and interrelationship between cyberspace and the information environment. The distribution of information and data, their timeliness and quantity are directly dependent on the capabilities and limitations of the network infrastructure.

Easy access, the complexity of networks and applications, lack of security considerations in network design and application development, inadequate user activity give cyberspace the *characteristic of vulnerability*. Access to cyberspace by an individual or group of individuals who own a network device is easy, and an individual with a single device may be able to disable an entire network. The vulnerability of systems operating in cyberspace requires that measures be taken to reduce risks and protect cyberspace. The effects generated in cyberspace can have a global impact on physical domains.

Understanding the vulnerabilities and components of the operational environment allows the decision to be relevant, context-related. The continuous application of these analytical frameworks allows the commander and staff to analyse the cyberspace from different perspectives throughout the operational process.

CONCLUSIONS

Cyberspace is playing an increasingly important role in leading the armed fight. Some cyberspace actions are ongoing, regardless of the existing alert state or the occurrence of a conflict. Defence and security cyberspace actions must be a constant concern of specialised structures and must also be in the attention of commanders of all structures. The new weapons systems, in addition to offering numerous operational advantages, also present vulnerabilities due to the interconnection with cyberspace.

Cyberspace plays an important role in the planning process, and if used properly, actions planned and carried out in this environment can replace some of the effects of other types of military action involving high resource consumption. As a specificity of the operational environment, there is the time when hostile actions are carried out - long before the official launch of the other operational environments.

Therefore, the process of cyberspace operations planning may not take place at the same time as the planning of the operation to be performed.

BIBLIOGRAPHY:

1. Azmi, R., Kautsarina, K. (2019). *Revisiting Cyber Definition*. ECCWS 2019 18th European Conference on Cyber Warfare and Security, https://books.google.ro/books/about/ECCWS_2019_18th_European_Conference_on_C.html?id=b8-hDwAAQBAJ&redir_esc=y, retrieved on 22 September 2020.
2. Barber E.D., Bobo T.A., Sturm P. K. (2015). *Cyberspace Operations Planning: Operating a Technical Military Force beyond the Kinetic Domains in Military Cyber Affairs*. The Journal of the Military Cyber Professionals Association. Vol. 1, no. 1, art. 3, https://core.ac.uk/download/pdf/71958458.pdf, retrieved on 24 September 2020.
3. Emmott, R. (2018). *NATO Cyber Command To Be Fully Operational in 2023*, https://www.reuters.com/article/us-nato-cyber/nato-cyber-command-to-be-fully-operational-in-2023-idUSKCN1MQ1Z9, retrieved on 24 September 2020.
4. ADP 2-0, *Intelligence*, 2019.
5. Congressional Research Service (4 June 2020). *Intelligence, Surveillance, and Reconnaissance Design for Great Power Competition*, https://crsreports.congress.gov, retrieved on 12 September 2020.
6. FM 3-12, *Cyberspace and Electronic Warfare Operations*, April 2017.
7. FM 3-38, *Cyber Electromagnetic Activities*, February 2014.
8. *Decision no. 271/2013 to Enforce Romania's Cyber Security Strategy and the National Action Plan on the Implementation of the National Cyber Security System*. Government of Romania, 23.05.2013.
9. *Joint Publication 3-12, Cyberspace Operations*, 8 June 2018.
10. *Moore's Law and the Future of Mathematics*, https://rum.journal-headerpop.com/make-mine-double-moores-law-824535, retrieved on 14 August 2020.

WEBOGRAPHY:

1. https://www.cybercommand.ro, retrieved on 15 September 2020.
2. https://www.defenseone.com/technology/2019/05/nato-getting-more-aggressive-offensive-cyber/157270/, retrieved on 13 September 2020.

3. https://intelligence.sri.ro/evolutia-amenintarii-cibernetice/, retrieved on 26 September 2020.
4. https://www.reuters.com/article/us-nato-cyber/nato-cyber-command-to-be-fully-operational-in-2023-idUSKCN1MQ1Z9, retrieved on 10 September 2020
5. https://rum.journal-headerpop.com/make-mine-double-moores-law-824535, retrieved on 21 September 2020.

SHAPING THE OPERATIONAL ENVIRONMENT THROUGH CYBERATTACKS

Lieutenant Colonel Marian ȘTEFAN

Defence Intelligence Training Centre, Bucharest

The current geopolitical and geostrategic context, the scale of politics, economics, culture and religious interests, information and cyber problems, the global medical crisis, as well as other non-military measures nowadays occupy a special place in shaping the operational environment. Their importance is felt not only during the escalation of crisis situations and their management and control, but also in military operations, marking the architecture of contemporary conflicts. A variety of present and involved actors, together with the multitude of risks and threats they generate, change the paradigm of the classic operational environment, towards multidimensional operational approaches in relation to the five traditional dimensions we are already familiar with from the military literature: land, air, sea, space and the electromagnetic spectrum, to which now the environment and the information environment are added. Overlapping these environments and creating an integrated battlespace image is a paradigm shift that must be understood and assumed. Social platforms and information warfare, artificial intelligence and self-learning programmes used in the military environment redefine the future security environment and the operation environment both in peacetime and in situations of crisis or at war.

This study proposes a holistic presentation of the problems and challenges at the level of the international operational environment, presenting different typologies of threats identified at the level of the informational component by instrumenting cyberattacks attributed to state and non-state entities. The shaping of theoretical concepts is accompanied by a series of examples presented in order to provide a detailed perspective on events that have affected the information environment.

Keywords: environment operational; cyberattacks; aggressions; crisis; technology;

GENERAL NOTIONS

The broader way of approaching security has lately acquired a new type of components, initially coined *"non-traditional threats"*, and afterwards *"emerging security threats"*, because NATO has considered them to be very important, thus stepping on a new and uncertain territory. This area of threats includes terrorism, proliferation of weapons of mass destruction, cyberattacks, power and power assets supply outages: *"The evolution of international relations, the turmoil and the acceleration of the integration and fragmentation of the World International Order have led to unexpected and unconventional forms and types of threats to national and international security. Some of these threats stem from the process of technological development, others from the impact of technology on our society, others from the growing populism and relevance of identities, and last but not least, the ones generated by our own minds and perceptions, dramatically influenced by our preconceptions and the inclination to seek the easiest ways in rational thinking. All this has an enormous impact on security and national defence threat assessment. Therefore, these factors must be explored, known and addressed in a scientific and comprehensive manner, in order to prevent strategic surprise in these areas, as well as the emergence of new types of conflicts"* (Chifu, 2020, p. 10).

Although the world we live in is constantly experiencing new technological developments, the speed of evolution of our society, international relations and security has created new categories of unconventional threats. In this way, threats from external sources are correlated with internal vulnerabilities that are also transformed into threats. This happens because, in reality, they correspond to the typology of hybrid threats, which are generated by external sources (Chifu, 2018, pp. 23-30). This is the case for all the features of liberal democracy, the values and principles we respect because they represent our way of life, but which are considered vulnerabilities by certain actors (state actors, especially by the Russian Federation and China, and non-state ones, entities and terrorist organisations, organised crime groups), which have built tools to take advantage of them (Chifu, Țuțuianu, 2017, p. 270).

The new types of threats come from speculating on the principles and values of the democratic system of government, taking advantage of the shortcomings and ambiguities identified in these systems, generated by the evolution of technology and its impact on society (Chifu, 2019, pp. 11-23).

Social media and information warfare, artificial intelligence and the use of self-learning programmes in the military environment redefine the future security environment and the operating environment. The most profound changes come from the area of advanced technologies with freedom of action and decision-making.

The geopolitical and geostrategic context, the scope of political, economic, cultural and religious interests, information and cyber problems, as well as other non-military measures occupy nowadays a special place in shaping the operational environment. Their importance is felt not only during the escalation of crisis situations and in the process of crisis management and control, but also in military operations, marking the architecture of contemporary conflicts.

The array of present and involved actors, together with the diversity and scale of risks and threats they generate, change the paradigm of the classical operational environment towards multidimensional operational approaches, in relation to the five traditional dimensions we were familiar in military literature: land, air, sea, space and the electromagnetic spectrum, to which the surrounding environment and the cyber environment are now added. Overlapping these environments and creating an integrated battlespace image is a paradigm shift that must be understood and assumed.

In terms of the traditional approach, US military doctrines extend the list of components of hybrid threats to include *"two or more of the following: military forces, national state paramilitary forces (such as internal security forces, police or border guards), insurgent organisations (movements that primarily rely on subversion and violence to change the status quo), guerrilla units (irregular indigenous forces operating in occupied territory), criminal organisations (such as gangs, drug cartels or hackers)"* placing a strong emphasis on the use of information and cyber operations (TRADOC G-2, 2012, p. 5). This picture of the current operational environment specific to hybrid warfare, including combinations of conventional and irregular forces, provides a perception limited to military warfare tools, along with elements of organised crime and cyberattacks. For a historical study of military campaigns, such an approach may be useful, but to explain the combination of military and non-military power tools used to achieve a state's strategic objectives, this is not enough. The tacit nature of the conflict in cyberspace makes it difficult to distinguish between the origins and triggers and the end state desired by the actors who triggered the aggression.

THE INTERNATIONAL CONTEXT OF THE OPERATIONAL ENVIRONMENT

The global operational environment is characterised by the existence of two main phenomena. First of all, there is an increasingly acute phenomenon of power vacuum generated by states with fragile or failed systems of governance, which, through the vulnerabilities created, enables the rise of non-state actors through their asymmetric or hybrid nature, generates security crises at the state or even regional level. Increasing the number of well-organised, armed and funded non-state actors poses threats to security and sovereignty at the level of weakly governed states. These interferences in the governing act of non-state actors manifest themselves in two ways: on the one hand, they can position themselves as a possible alternative to the traditional form of government based on the rule of law and recognised, but failed state structures, given the taken measures and exercised policies, and on the other hand they can challenge, by the nature of their existence and presence, the monopoly of the force structures of the host state.

The second important phenomenon that manifests itself in the current medium-sized operation is represented by strategic competition (struggle for different resources, markets, areas of influence, geopolitical and geoeconomic interests) between strong states with conflicting interests.

The two phenomena may seem contradictory at first sight, but analysing the details and especially the common elements we find that in fact there is a connection: in situations where instability leads to the breakdown of existing elements of government, a state creates gaps in command structures and so-called *"open doors"* that regional or global powers, regional or transnational non-state entities can exploit to improve their positions or strengthen their influence.

The fragmentation of states was the main concern for international security in the decades after the end of the Cold War. Unlike the tense international security environment that existed during the Cold War, but stable in terms of the foreign policies of the two power blocs, the conflicts of the 1990s and 2000s were perceived as *"asymmetric"*, at least in terms of the use of unconventional elements. Thus, states with inferior and outdated military technical equipment, but innovative and adapted to the context of the operational environment have become formidable opponents for the armed forces of states that spend significant budgets for the defence industry, just because they knew the vulnerabilities of their opponents and managed to exploit them successfully. Although this phenomenon persists, we are now witnessing an increase in hybrid conflicts characterised by situations in which both classical and asymmetric threats are used in a combined manner. Innovative combinations of the use of conventional technologies and the products of new technological advances create a kind of dynamic and unpredictable conflict. The current operational environment blurs the distinction between war zones and peace zones, as well as between legitimate combatants, unassigned opponents and civilians.

One of the most critical dimensions of the hybrid conflict is the countering of military and political efforts at the same time with the overlapping use of information aggression.

Information warfare is usually used in hybrid conflicts to create dissent in the public opinion of the population of the target state, to generate legitimacy of intrusive actions by fabricating a credible pretext, to prevent or slow down the response of the target state to kinetic and non-kinetic attacks and to reduce the chances of external interference by creating situations of legislative confusion. The most successful hybrid campaign is the one that paralyses the institutions of the target state and makes unavailable the ability to resist or react before the forced introduction of force – the nature of which can later be characterised as an instrument of stability (generators of peace and stability) instead of the instrument that created the instability. The control of all classical and modern media channels will lead to the possibility of using them in order to influence the internal public, and given that this control will be achieved from the initial state of conflict or in an incipient form, before any other actions, the effects will be to undermine the will of the target population to withstand further aggression. In situations where topics and messages constructed by the aggressor for the purpose of misinformation and intoxication have to compete with the international press and the unregulated Internet, the specific content of these launched topics is less important than saturating these areas with misinformation to help mask the aggressor's actions.

VULNERABILITIES OF THE INFORMATION ENVIRONMENT – THE TARGET OF CYBER AGGRESSIONS

Conceptually, a complex operational environment is composed of a multitude of actors who interact quickly, in different ways, being highlighted by structural complexity and interactivity. The levers that govern interactions are sometimes ambiguous and can be opaque to external actors without a deep understanding of the context. The characteristics of the conditions in an operational environment are constantly evolving, the information component being the most dynamic.

Part of the operational environment, the information dimension presents complexity, volatility, uncertainty, instability and ambiguity in events that change in speed, pace and tempo. A number of hybrid threats, including cyber-aggression, propaganda and influence, and misinformation spread in virtual environments, can extend the impact of planned military operations. Cyber-attacks pose an increasingly critical threat to information technology infrastructure and the ability to effectively execute a mission command. Any adversary will try to shape an operational environment to his advantage, changing the nature of the conflict and using capabilities for which any military force used is not fully prepared.

An information system, in general, can be defined as the set of elements involved in the process of collecting, transmitting and processing information, which has a central role in this system. The information system includes the following components: spread information, documents carrying information, personnel who have access to information, means of communication, information processing systems (usually, automatic) etc. Some of the activities carried out within this system involve: the acquisition of information from the basic system, the completion of documents and their transfer between different compartments, the centralisation of data etc. In the broadest sense, any information system refers to the various interactions between people, data, processes, and technologies. In this way, the term does not only refer to the aspects related to information and communication technologies that an organisation uses, but also to the way in which people interact with the technology in order to provide support for processing processes. The information system represents a complex set of data flows and information circuits organised in a unitary conception.

The development of information and communication technologies over the last 20 years has served as a powerful and accelerating catalyst for changing the distribution of power in the international system, as well as how to use it. The dominance of related technologies is increasingly changing the physiognomy of the current operational environment, as technological capacity and economic power invested in the military sector are closely linked. The emergence of cyberspace has added new ground for conflicts between states of the world or between non-state organisations. In terms of global governance and the right balance between individual freedom and state control, the challenges are growing as states' monopoly on certain types of information has been eroded in favour of individuals and non-state actors. The technological revolution is disrupting military concepts and doctrines in ways that seem to reduce the contribution of the human factor in the event of conflict and diminish some of the advantages that Western armed forces had at the end of the Cold War.

Information and communication technologies shape all the power tools of states, including diplomacy, information and the use of force. Advances in technology and the digitisation of information have made it possible to collect information more intelligently and the emergence and involvement of a wide range of actors. The existence of a large volume of information stored in databases controlled by large private concerns is inherently viewed as insecure by Western governments, while social media content serves as a repository of personal information about potential information targets that have so far remained untouched for state institutions. The great powers have a significant advantage in controlling information, but any state with a telecommunications agency has the ability to develop ways to collect such signal information – SIGINT. China is a prime example of a state whose information gathering, processing and storage capabilities have been dramatically transformed over the past 20 years through the use of cyber espionage for both commercial and military purposes. Many countries in Africa, Asia and Latin America use improved collection capacities to more effectively monitor or repress dissent among their own populations. Meanwhile, North Korea has used its substantial cyber capabilities to attack both its opponents and its revenue from cybercrime, a case of the theft of US $ 81 million from the central bank of Bangladesh in 2016.

The fact that espionage levels have become so ubiquitous has probably created a new and unprecedented set of circumstances. It has often been observed that when it comes to digital networks, the distinction between espionage and sabotage can only be determined by intention. This is not strictly true, given that any digital exploitation aimed at espionage will necessarily have a specific sabotage component. There will always be a fear that any discovered exploitation – and the average discovery time can range from 146 days in the US to over 400 days in the EU (www.iiss.org/publications/strategic-survey) – can have a sabotage component that is too sophisticated to be easily identified. States are increasingly using their intelligence capabilities (both in the form of state agencies and non-state entities) to penetrate enemy networks in order to identify vulnerabilities that can be activated in time of tension or conflict, in order to affect the functioning of the company itself. Such exploitations may also have a signalling function, designed to discourage states from taking hostile actions for fear of a harmful response.

This is a challenge for decision-makers both in states engaged in cyber espionage and in those that are targets of such activities. The picture is still quite blurry,

with the risk of undesirable consequences, as in 2017 NotPetya, a highly virulent ransomware virus, mainly directed against Ukrainian government agencies, spread widely in Australia, Europe, Russia and the US, causing billions of dollars in damage. The CIA has attributed the GRU virus to Russia's military intelligence agency, which appears to have used the conflict with Ukraine as a test ground for a number of cyber exploits. The impact of such exploits highlights the so-called *"connectivity paradox"*, whereby the most advanced network-dependent technologies are also the most vulnerable to significant cyber disruptions.

Such disruptions are becoming a familiar part of a new approach to competition between states, in the form of what has been called grey area operations. These operations were described by the US Special Forces Command as *"a competitive interaction among between and within state and non-state actors that falls between the traditional war and the state of peace"* (Special Operations Forces within the Competition Continuum, 2020). They are characterised by ambiguity about the nature of the conflict, the opacity of the parties involved and uncertainty about the relevant policies and legal frameworks. There is nothing intrinsically new about such operations, but the development of technologies has greatly facilitated them, allowing actors to undertake (at low cost and with the possibility of denying) a series of activities that cause damage without amounting to a level that would easily justify a kinetic response. An example of this type of operation is the attacks by entities that acted on behalf of the Iranian state between 2011 and 2013 against the US banking and financial system, undertaken in response to US sanctions related to the Iranian nuclear program.

The most eloquent example is Russia's alleged interference in the 2016 US presidential election, which focused on the exploitation of social media platforms. Russians claiming to be US citizens have opened a large number of fake social media accounts, predominantly on social media platforms Facebook and Twitter. These accounts were used to spread messages focused on social issues at the time, which were then amplified by robots (software applications that perform simple repetitive tasks at a much faster rate than humans can). This created the impression of a real national debate on certain issues of interest, from immigration and racial issues to the behaviour of candidates in the election campaign. In this way, American politicians felt compelled to address the issues of debate and the traditional media in order to fill the void of credible information, thus creating a further amplification of false propaganda. A few days before the election, Russian hackers also tried to hack into the US voting systems by sending malware-infected emails to state election officials' computers.

The objectives of this Russian campaign evolved from an initial intention to discredit one of the presidential candidates and to generate distrust in the US political process to promote the candidacy of the other politician, considered the most suitable person to raise or lower sanctions on Russia. This approach exemplifies the Russian concept of reflexive control, defined as *"a means of transmitting to a partner or adversary information specially prepared to voluntarily incline him to take the predetermined decision desired by the initiator of the action"* (Kowalewski, 2017). In fact, it has allowed Russia to cause significant damage to the integrity of the US democratic process at minimal cost by digitally exploiting existing cracks in American society, using computer systems available to the general public and home users. Although the US government was well aware of what was happening and who was responsible, its ability to respond to such behaviour in a timely manner or to effectively sanction such actions was limited.

Although China has not yet tried to mimic the type of information operations used by Russia, the state has used technological advances in research in this area to expand its influence in a variety of ways to shape the operational environment in its own interests. In the international diplomatic arena, China has taken on the role of supporting the concept of cyber sovereignty and the need for new forms of global governance of the cyber realm. China's cyber operations reflect a continued focus of state intelligence agencies' efforts on espionage, with some coercive intentions as a secondary objective.

Unlike China, Iranian cyber activity is much more focused on retaliation against regional and Western neighbours than serving a direct coercive purpose. Cyberattacks on Saudi oil companies began with a destructive attack in 2012, which destroyed about 30,000 computers in the networks of the Saudi state oil company (ARAMCO), but did not have a noticeable impact on oil operations. In 2017, the same malware caused similar damage to the petrochemical company Tasnee; that attack was followed by a subsequent attack on ARAMCO in August 2017, involving TRITON intrusion malware.

The information environment is a construction based on the idea that the existence and proliferation of information systems create a distinct dimension or operating environment. As a combination of tangible elements (physical information systems and networks) and intangible elements (information and decision-making), the information environment is both a resource for military operations and an environment in which the armed forces operate. In any operational environment, the intangible element, information, is of paramount importance. This is because, despite its lack of physical existence, the content and flow of information in a specific geographical area produce real, tangible effects on the physical world and on the military forces present in the operating environment. For these reasons, the understanding of the information environment must ultimately include how the content and flow of information affect the conduct of military operations.

Finding the author of cyberattacks is difficult, requiring a process of collecting large volumes of information, analysing them, and making a decision to identify who is responsible. Very rarely do the traces left by a cyberattack provide clear evidence for IT specialists so that the source of the attack, either a state institution or a person, can be indicated in order to be able to provide evidence in a court of law.

The proliferation of information and communication technologies, both in terms of the widespread use of these technologies and the increased availability of destructive means, have generated new ways of projecting power tools (Paleta et al, 2008). Political and economic differences between states now involve solutions through cyberattacks on the utilities, financial networks, electoral infrastructure and governance systems of other countries. Cyberattacks that involve the deliberate use of a software product specially designed and targeted to exploit or modify computer code, data, or algorithms to cause damage provide new ways to target Internet infrastructure, telecommunications networks, information systems, and computers and computer systems. Such activities could be aimed at destroying or affecting the proper functioning of these systems with negative effects on their users, whether they are states, companies, public service providers or individuals.

CONCLUSIONS

The United Allied Doctrine for Information Operations defines the information environment as one that *"includes information, actors and systems that allow the use of information"* (AJP-3.10, 2009, p. 1-1). In this context, the information environment has become the system in which entities, means of communication, communication systems and volumes of data transmitted act simultaneously for a single purpose, communication. The distances between information generators and receivers or users have dissipated with technological development, so that the ideas promoted by anyone in the virtual environment can be accessed instantly by using a wide range of terminals or computer systems, thus becoming a global issue. The global information environment has the advantages of advanced technologies, offers unlimited access to resources, but is a vulnerable space in the face of cyber aggression. Basically, this double-edged sword offers government entities and individuals as well niches of penetration and ways to convey data of a disinformation nature. *"Information warfare, according to a definition of the concept, is the creation of alternative realities by perverting the truth based on real data, facts and arguments and interpreting it by using a combination of facts, syllogisms, sophistry, propaganda, forced interpretation and a multitude of lies. Alternative reality perverts the perception of a target population, in a combination of psychological operations – PSYOPS, along with misinformation and propaganda, using fundamental beliefs, feelings and strong images, in order to lead the target audience to a pre-defined perception"* (Chifu, 2015).

BIBLIOGRAPHY:

1. Chifu, I. (2015). *Război hibrid, Lawfare, Război informațional. Războaiele viitorului*. "Strategii XXI" International Scientific Conference. "The Complexity and Dynamism of the Security Environment". Bucureşti: Centrul de Studii Strategice de Apărare şi Securitate.
2. Chifu, I., Țuțuianu, S. (2017). *Torn between East and West: Europe's Border States*. London and New York: Routledge Publishing House.
3. Chifu, I. (2018). *Războiul hibrid şi reziliența societală. Planificarea apărării hibride*. In *Infosfera Review*.
4. Chifu, I. (2019). *Technology and Democracy. The Impact of the Evolution of Security and International Relations*. In "Strategii XXI" International Scientific Conference. Strategic Changes and International Relations. Bucureşti: Universitatea Națională de Apărare "Carol I".
5. Chifu, I. (2020). *Amenințări neconvenționale și noile tipuri de conflicte de natură hibridă în secolul 21*. In *Gândirea militară românească* Journal, no. 1.
6. Kowalewski, A. (2017). *Disinformation and Reflexive Control: The New Cold War*, https://georgetownsecuritystudiesreview.org/2017/02/01/disinformation-and-reflexive-control-the-new-cold-war/, retrieved on 17 August 2020.
7. Paleta et al. (2008). *Information Technology and Communication and Best Practices in IT Life Cycle Management*. In Journal of Technology Management & Innovation, vol. 3, no. 4.
8. Williams, P. (2008). *Violent Non-State Actors and National and International Security*. International Relations and Security Network. Zurich: Swiss Federal Institute of Technology, http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?id=93880, retrieved on 15 August 2020.
9. AJP-3.10, *Allied Joint Doctrine for Information Operations*, 2009.
10. *The Global Risks Report 2016*, the 9th edition, http://www3.weforum.org/docs/GRR/WEF_GRR16.pdf, retrieved on 10 June 2020.
11. *The Impact of the ICT Revolution on International Relations* (2018), www.iiss.org/publications/strategic-survey, retrieved on 12 August 2020.

12. *Special Operations Forces within the Competition Continuum*, https://www.doctrine.af.mil/Portals/61/documents/Annex_3-05/3-05-D03-SOF-Competition-Continuum.pdf, retrieved on 13 August 2020.
13. TRADOC G-2. (2012). *"Operational Environments to 2028: The Strategic Environment for Unified Land Operations"*.
14. https://www.iiss.org/publications/strategic-survey/strategic-survey-2018-the-annual-assessment-of-geopolitics/ss18-04-strategic-policy-issues-2, retrieved on 11 June 2020.
15. https://www.globalpolicy.org/nations-a-states/failed-states.html, retrieved on 11 June 2020.

THE MILITARY LEADER COMPETENCIES AND ATTRIBUTES IN A MILITARY ORGANISATIONAL CONTEXT

Major Assoc. Prof. Alexandru BABOȘ, PhD

"Nicolae Bălcescu" Land Forces Academy, Sibiu

Lieutenant Colonel Assoc. Prof. Paul TUDORACHE, PhD

"Nicolae Bălcescu" Land Forces Academy, Sibiu

The military requires that leaders should make the right choices, often in critical situations, and establish a unique and inclusive vision for the organisation. Military leaders must always take responsibility for the conduct and management of missions, provide the purpose, direction and motivation needed to carry them out and improve the organisation. In order to succeed in fulfilling these desiderata, a series of correlated actions are necessary, the amount of which is transposed in the competences of the military leader, so necessary in the totality of the military actions.

Keywords: leadership; leader; skills; developing others; building trust;

INTRODUCTION

Military organisations, with a similar level of technical procurement and human resources, with standard organisational structures, obtain different results. This is mainly due to those in leadership positions, the leaders, who use specific methods of communication and resort to different means, other than the usual patterns. The one in the leadership position, who manages to obtain the emotional and voluntary participation of all the members of the organisation of which he is part, is an authentic leader, and the act of leadership (command) becomes a service, that of leadership. The qualities of the leader, leadership, motivation in work and communication are decisive in achieving the coordination and training of subordinates.

All this, valid in any type of organisation, can also be valid in military organisations. The term *leadership* basically refers to an abstraction, a synthesis of theories and practices of influence and power in organisations. In the literature, prestigious social positions that allow the possibility of interpersonal influence designate the field of leadership, and individuals who occupy these positions are called leaders.

Leadership is the complex process by which the leader of an organisation leads and trains subordinates, through non-coercive means, in a direction that will lead to the realization of its long-term interests (Covey, S., 1995, p. 23).

The role of the leader in the leadership process is expressed by his personality, motivations and skills and legitimacy. *Subordinates*, in turn, contribute with their personality, skills and expectations to the situation. *The situation* is determined by certain resources, tasks, structures and rules specific to military life. In the area where these three variables overlap, we meet leadership (Covey, S., 1995, p. 32).

Leadership is a process of influence, and effective, good leadership does not appear randomly, but involves a skill/competence that can be developed. A leader influences other people/subordinates to accomplish a mission or achieve a goal. Means of influence include actions aimed at transmitting and multiplying motivation among subordinates. The leader is responsible not only for fulfilling the current mission, but also for the continuous development of subordinates and generating change in the organisation in order to improve long-term activity (TLS5, 2017, p. 1-1). The effective leader must be able to handle situations effectively, achieve individual, group or organisational goals. The effectiveness of the leader is measured by how one or more of these goals are achieved. Individuals may perceive the leader as efficient or inefficient, depending on the benefits obtained from the activity performed (Zlate, 2004).

In the dynamic approach to the natural group, K. Lewin defined the leader as *“the person who at some point allows the group to develop its dominant need or needs”* (Abric, 2002).

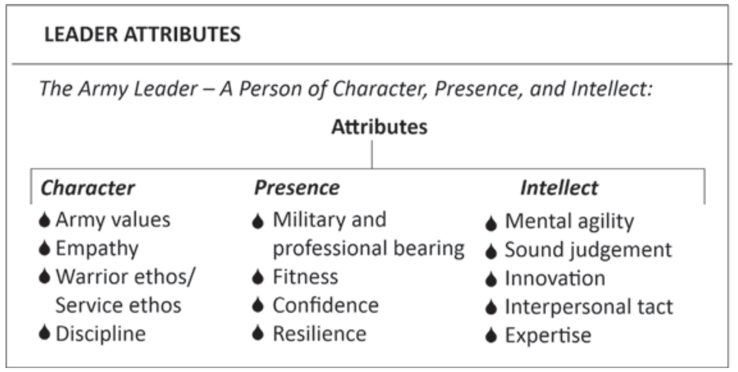
The effective leader must be able to handle situations effectively, achieve individual, group or organisational goals. The effectiveness of the leader is measured by how one or more of these goals are achieved. Individuals may perceive the leader as efficient or ineffective depending on the satisfaction they get from the work done (Zlate, 2004). The leader is *“the person who administers (leads) or guides (directs) others”* (Dictionary of Human Resource, 1997, p. 139), the person who exercises power has a great influence within social groups of various sizes (Zamfir, 1998, p. 328); the person who achieves outstanding results with a certain effectiveness in any field of activity, regardless of the obstacles that might occur.

The quality of leadership exercised is influenced by the leader’s ability to acquire the power associated with the formal position and the way he/she uses it in the process of influencing the behaviour of subordinates. In fact, power itself comes from the will of subordinates to follow the direction indicated by the leader and from his/her ability to meet the needs of subordinates. When present, leadership produces change.

In peacetime, the army can perform the functions for which it was created through good administration and management. However, in case of a military confrontation, the correct administration and the specific management of peace are insufficient (Arădăvoaice, 1998). In war, there is a need for authentic, efficient leaders, at absolutely all levels of the army structures. The need for such leaders in the military organisation is supported by the obligation of adaptability and ability to respond to changes in the environment, as well as organisational flexibility. At the same time, they contribute decisively to the stability and cohesion of the organisation.

LEADERSHIP ATTRIBUTES

Considered to be internal characteristics of a leader, the attributes of leadership can be the person’s beliefs, empathic capacity, character aspects, ways of expression, action, etc. (ADP 6-22). In the military organisation, a leader who fully accepts and finds himself in the values and characteristics of the military profession, associated with the specific competencies of leadership, will be an authentic and positive leader.



LEADER ATTRIBUTES

The Army Leader – A Person of Character, Presence, and Intellect:

Attributes

Character	***Presence***	***Intellect***
♦ Army values	♦ Military and professional bearing	♦ Mental agility
♦ Empathy	♦ Fitness	♦ Sound judgement
♦ Warrior ethos/ Service ethos	♦ Confidence	♦ Innovation
♦ Discipline	♦ Resilience	♦ Interpersonal tact
		♦ Expertise

Figure 1: Leader attributes (ADRP 6-22, 2012)

The attributes of the leader relate to the way they behave and learn in the environment in which they operate. The attributes of the leader in a military organizational context are character, intellect and attitude (TLS5 Smartbook, 2017). More specifically, the values and identity of the leader (character), the external image of the leader, the behaviour, communication (attitude) and the social ability that the leader uses in the act of leadership (intellect). A good character, a solid attitude and a fine intellect allow those skills necessary for the leader to be exercised with maximum effect.

Integrity is a key element of a leader’s character, because it means doing what is right, moral and legal, by applying objectivity and fairness in the exercise of leadership. Fair leaders adhere to the values of the organisation to which they belong, and combine them with those of personal identity in order to set standards for their subordinates. Thus, the immediate effect will be demand and, last but not least, *availability*. Leaders identify with their role and expectations from their subordinates and assume full responsibility for all activities undertaken.

We often hear the phrase *“first impression matters”*, regardless of the specifics of the organisation we belong to. However, in the case of leadership, these words have a greater impact, because the impression that leaders make on their subordinates, as part of the process of influencing, contributes to the success of the legitimacy of the position they hold. *Attitude* is basically a projection of military and professional attire and conduct, of the leader’s self-confidence, of adaptability (TLS5, 1-19).

The intellect influences the way the leader analyses the problems that arise, finds solutions and makes decisions. Every leader must be realistic, know their limits and use them properly. Mental agility helps leaders cope with any change, adapt to any situation and to the dynamics of operations. A sound judgment makes it possible to take the best decision and facilitates both understanding and executing it in the best possible way.

THE MILITARY LEADER COMPETENCIES

Competence is defined as the ability of the individual to integrate into requirements by producing results with projected qualitative characteristics (Dubois, 1993). Another definition of competence would be that it is an inherent characteristic of the individual (motivation, character trait, quality, aspect of self-image, social role or set of knowledge) that allows him to achieve a higher level of professional performance (Boyatzis, 1982).

Competence also implies certain knowledge, skills, aptitudes, professional capacity attested by diplomas and certificates from educational institutions, seniority in work, decision-making capacity, etc. Competence assumes to be the only criterion by which to capitalise the entire activity of a person or members of a community.

The need for leaders necessarily stems from the state of insecurity and uncertainty that characterises the military organisation during the fulfilment of its constitutive mission (Sfârlog, 2005, p. 53). Leadership is associated with vision. In order to translate vision into reality, leaders must possess specific competencies that guide their actions. Competencies are understood as a set of talents, knowledge and abilities that make a person suitable or well qualified for a position within the organisation.

Researchers in the field consider that three main sets of competencies are needed, namely *internal competencies* (leadership foundation), *leadership competencies* (to differentiate between leaders and bosses) and *professional competencies* (derived from experience, learning, training). Together, they constitute the *Pyramid of Leadership*.

The leader's competencies develop from a balanced combination of studies, self-development abilities, training and professional experience (TLS5, Leader Competencies, 1-33). Competencies provide a clear and consistent direction that expresses expectations from military leaders. Leaders' competencies can be built up as they reach higher strategic hierarchical levels within the military organisation. Hence, leaders constantly develop their ability to exercise these competencies as effectively as possible and apply them in increasingly complex situations. A possible model of leadership competencies, practically of expectations from leaders, is illustrated in *figure 3*.

According to ADRP 6-22, *Army Leadership*, there are three categories of competencies: leading others, developing themselves (developing others, the organisational environment and the military profession as a whole) and achieving organisational goals.

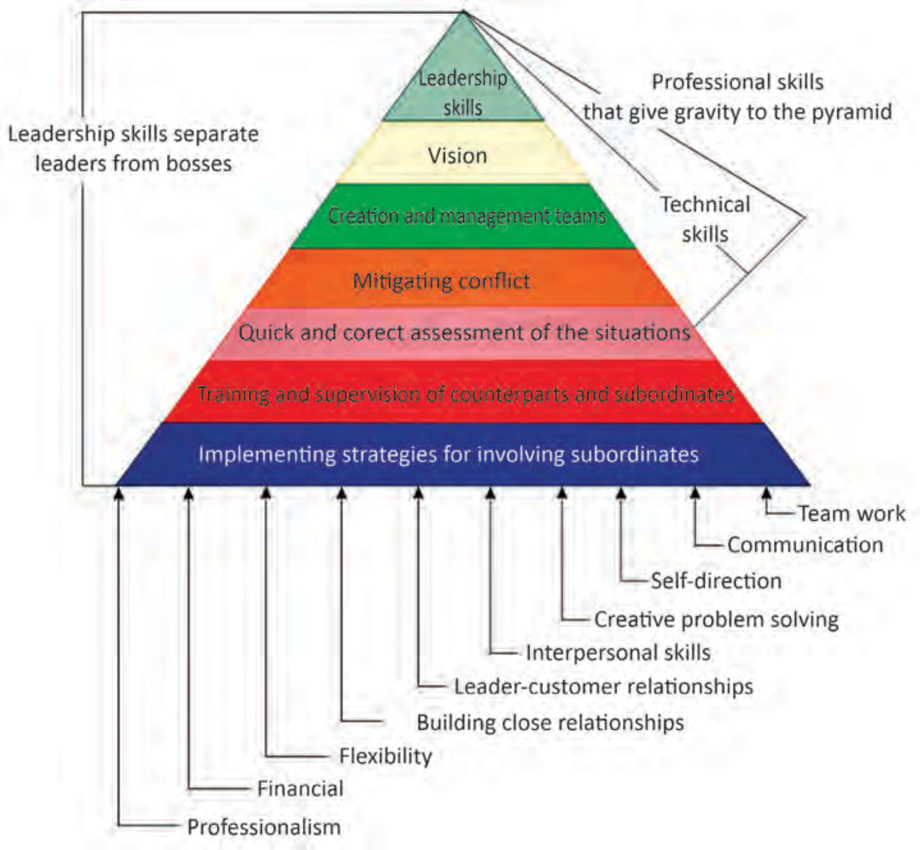
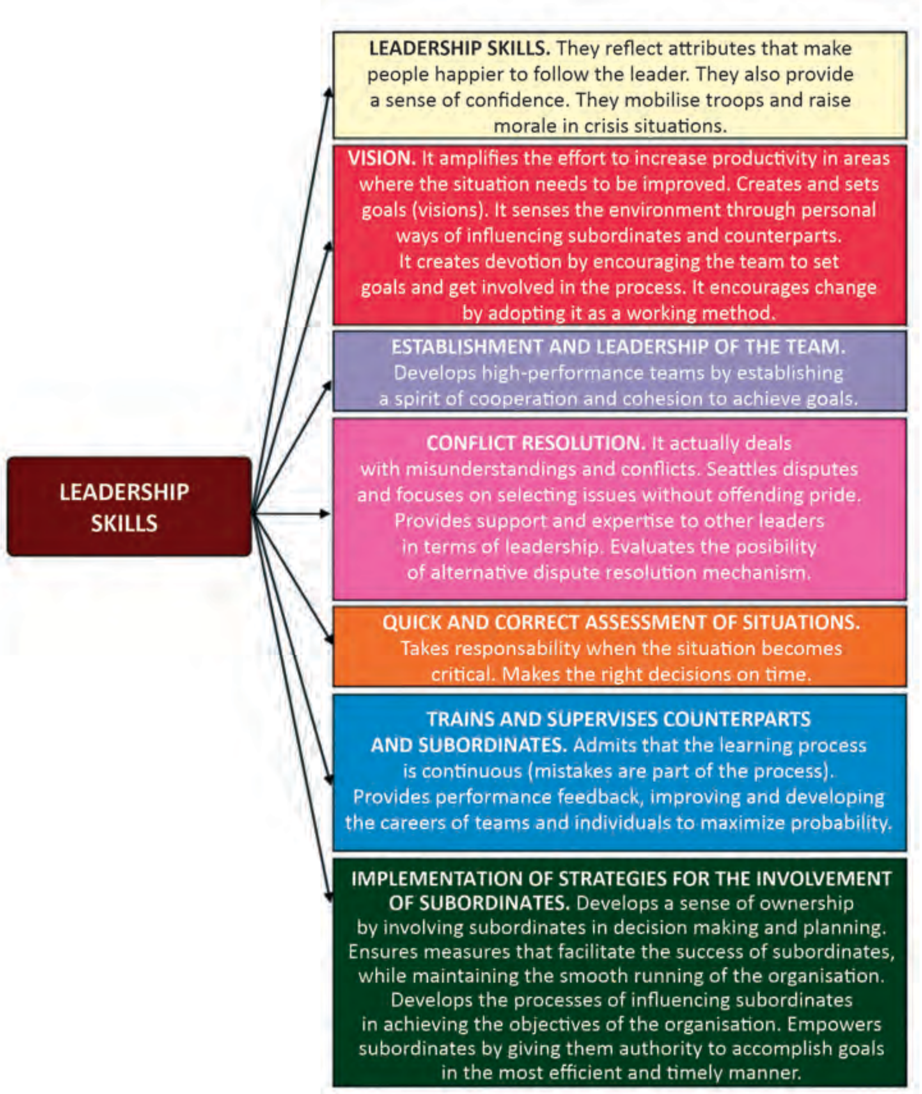

Leadership skills
Vision
Creation and management teams
Mitigating conflict
Quick and corect assessment of the situations
Training and supervision of counterparts and subordinates
Implementing strategies for involving subordinates
Leadership skills separate leaders from bosses
Professional skills that give gravity to the pyramid
Technical skills
Team work
Communication
Self-direction
Creative problem solving
Interpersonal skills
Leader-customer relationships
Building close relationships
Flexibility
Financial
Professionalism

Figure 2: Leadership pyramid (Sfârlog et al, 2010)

When discussing leadership, it is essential to emphasise aspects regarding the *influence* on subordinates, both military and civilian, as well as their *affiliation* to organisational values and goals. In order for the influence to have the desired effect and to increase its efficiency in conducting the target activities, and in order to create a positive working climate, it is necessary for the leader to build *trust* among subordinates. Exceptional leaders know that actions can be stronger than words, so many adopt a leadership style using their personal example, thus setting high standards for their subordinates. These leaders are expected to expand their influence beyond the chain of command, which involves communication, negotiation and conflict management skills. They must be able to identify whom to influence, and then what leadership functions to employ.



LEADERSHIP SKILLS

LEADERSHIP SKILLS. They reflect attributes that make people happier to follow the leader. They also provide a sense of confidence. They mobilise troops and raise morale in crisis situations.

VISION. It amplifies the effort to increase productivity in areas where the situation needs to be improved. Creates and sets goals (visions). It senses the environment through personal ways of influencing subordinates and counterparts. It creates devotion by encouraging the team to set goals and get involved in the process. It encourages change by adopting it as a working method.

ESTABLISHMENT AND LEADERSHIP OF THE TEAM. Develops high-performance teams by establishing a spirit of cooperation and cohesion to achieve goals.

CONFLICT RESOLUTION. It actually deals with misunderstandings and conflicts. Seattles disputes and focuses on selecting issues without offending pride. Provides support and expertise to other leaders in terms of leadership. Evaluates the posibility of alternative dispute resolution mechanism.

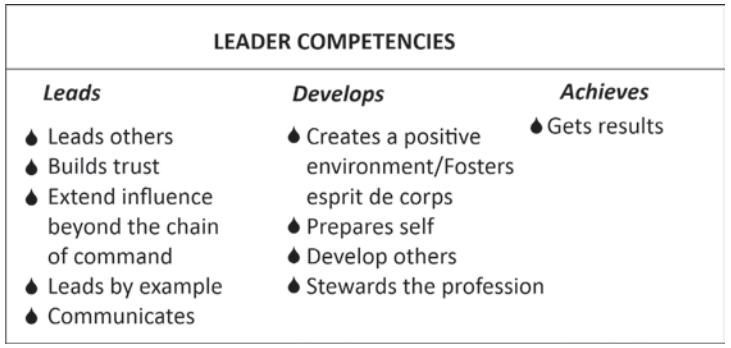
QUICK AND CORRECT ASSESSMENT OF SITUATIONS. Takes responsability when the situation becomes critical. Makes the right decisions on time.

TRAINS AND SUPERVISES COUNTERPARTS AND SUBORDINATES. Admits that the learning process is continuous (mistakes are part of the process). Provides performance feedback, improving and developing the careers of teams and individuals to maximize probability.

IMPLEMENTATION OF STRATEGIES FOR THE INVOLVEMENT OF SUBORDINATES. Develops a sense of ownership by involving subordinates in decision making and planning. Ensures measures that facilitate the success of subordinates, while maintaining the smooth running of the organisation. Develops the processes of influencing subordinates in achieving the objectives of the organisation. Empowers subordinates by giving them authority to accomplish goals in the most efficient and timely manner.

Figure 3: Leadership competencies (Ibid.)

Effective leaders try to continually improve the organisation they belong to, make it much better than when they found it, and expect those who will follow to do the same (ADRP 6-22, Army Leadership, chap. 7). A leader shapes the environment in which they and the others (the subordinates) operate. Strategic leaders shape the entire military environment, as well as the major defining elements of the various social categories or communities that operate within it. Leaders who have direct contact with the military shape the environment and culture at the unit level.



LEADER COMPETENCIES		
Leads	***Develops***	***Achieves***
♦ Leads others ♦ Builds trust ♦ Extend influence beyond the chain of command ♦ Leads by example ♦ Communicates	♦ Creates a positive environment/Fosters esprit de corps ♦ Prepares self ♦ Develop others ♦ Stewards the profession	♦ Gets results

Figure 4: Leader competencies (TLS5, 2017)

Both types of military leaders do so with the aim of streamlining the activities undertaken and driving the organisation towards change.

Regardless of the field of activity, *professionalism* is the main dimension of modern leadership, the basic prerequisite for achieving performance and fulfilling people's personalities. As opposed to amateurism, dilettantism, superficial work just *"for the sake of the boss"*, it is defined by *"Excellence"* (Arădăvoaice, 2014). Military professionalism is in demand today more than ever, as combat techniques, equipment and command systems are increasingly diversified, and the tactical, operational and strategic forms and methods of combat are complex and require knowledge in various fields. The variety of missions to be carried out by the military in times of peace, war, crisis situations, peacekeeping or humanitarian missions, on or outside the national territory, in cooperation with other armies, actively involve commanders, staffs and soldiers on multiple levels. The well-thought-out and well-done work, conducted promptly and with maximum efficiency, with minimum human and material losses, is the essence of the professionalism of today's military. Professionalism remains the linchpin that ensures the cohesion of the organisation and guarantees performance and professional fulfilment (Huntington, 1957).

Regarding the competence of *achieving goals and obtaining results*, the leader is responsible for prioritising, organising and coordinating the activities of the organisational structures, for identifying and allocating the necessary resources, for eliminating any obstacles that may hinder the accomplishment of the task. At the same time, the leader has a duty to recognize the performance, to appreciate/reward it accordingly, and to ensure permanent feedback as the work processes progress. Fulfilling the task or the entrusted mission in this way can only lead to the achievement of the objectives in an efficient way, which ultimately ensures the success of the leadership.

CONCLUSIONS

How leaders view their organisations heavily influences how they approach adaptation and lead those tasks. The key distinction from a leadership perspective is whether an organisation is considered in terms of a system outside of the people within it, or in terms of being responsive to the people within it. The former organisational culture based view leads to an organisation being considered in mechanistic terms that can be adapted in terms of refining or changing bureaucratic structures and decision-making procedures (Stacey, 2011). The tendency is that present leaders lean on the people within the organisation, which influences their leadership style and their adaptive capacity. Although a participative approach from the military leaders is desired, it is very hard to establish a common set of competencies and values required for them. The organisational culture itself, even if it is military, is so different from one nation to the other that it is very hard to establish a common military leader profile. In addition, the economic, social and cultural status of the nation can influence that. However, looking to the future and given recent technological and informational developments, a new set of competencies and a new military leader profile is required, that might put the *technical* competencies ahead from the social ones, or emphasise the *critical thinking* part more than problem solving skills.

BIBLIOGRAPHY:

1. Abric, J.C. (2002). *Psihologia comunicării*. Iaşi: Editura Polirom.
2. Arădăvoaice, G. (1998). *Managmentul organizaţiei şi acţiunii militare*. Bucureşti: Editura SYLVI.
3. Arădăvoaice, G. (2014). *Liderul performant – fundamente psihologice*. București: Editura Militară.
4. Boyatzis, R.E. *The Competent Manager: A Model for Effective Performance*. New York: John Wiley and Sons.
5. Burbulea, E. (1984). *Psihologie și pedagogie militară*. București: Editura Militară.
6. Covey, S. (1995). *Eficienţa în 7 trepte*. Bucureşti: Editura ALL.
7. Dubois, D.D. (1993). *Competency – Based Performance Improvement: A Strategy for Organizational Change*. Amherst, HRD Press Inc.
8. *Dicţionar de conducere şi organizare*. (1985). Bucureşti: Editura Politică.
9. *Dictionary of Human Resource & Personnel Management*. (1997). Peter Colling Publishing.
10. Huntigton, S. (1957). *The Soldier and the State: The Theory and Politics of Civil-Military Relations*. Belknap Press.
11. Sfârlog, B., Ralea, M., Giurcă, D.F. *Leadership militar – curs*. Sibiu: Editura Academiei Forţelor Terestre „Nicolae Bălcescu".
12. Sfârlog, B. (2005). *Liderul militar şi inteligenţa emoţională*. Revista Academiei Forţelor Terestre *"Nicolae Balcescu"*, no. 2 (38). Sibiu.

13. Stacey, R.D. (2011). *Strategic Management and Organizational Dynamics. The Challenge of Complexity to Ways of Thinking about Organisations*. Pearson Education. London.
14. Zamfir, C., Vlăsceanu, L. (coord.). (1998). *Dicţionar de sociologie*. Bucureşti: Editura Babel.
15. Zlate, M. (2004). *Leadership şi Management*. Iaşi: Editura Polirom.
16. ADRP 6-22 (2012). *Army Leadership*. Headquarters. Department of the Army. Washington D.C.
17. ATP 6-22.1 (2015). *Army Team Building. Headquarters*. Department of the Army. Washington D.C.
18. FM 6-22 (2015). *Leader Development. Headquarters*. Department of the Army. Washington D.C.
19. TLS5. (2017). *Leadership and Training in a Complex World*. Smartbook, The Lightning Press.

IMPLICATIONS OF THE COVID-19 PANDEMIC ON MILITARY EXPENDITURE: NEW PERSPECTIVES ON EUROPEAN DEFENCE COOPERATION

Felicia ȘINCA, PhD Student

"Carol I" National Defence University, Bucharest

Prof. Toma PLEȘANU, BEng, PhD

"Nicolae Bălcescu" Land Forces Academy, Sibiu

The global economic crisis of 2008 has had a negative impact on defence budgets in most European countries. After 12 years of efforts taken for the economic recovery, the member states of the European Union are once again facing financial challenges caused by the COVID-19 pandemic. Defence budgets are once again in danger of being reduced, but at the same time the European Union needs more than ever to show unity and cooperation.

In the wake of the 2008 crisis, defence cooperation was one of the solutions adopted by EU member states to protect and strengthen their military capabilities. The development of multinational capabilities has proven to be more cost-effective than nationally sustained efforts. The current situation, generated by the COVID-19 pandemic, reminded us that cooperation initiatives need continuous adaptation to the evolution of new types of crises. The planning, development, procurement, operation and support of joint defence equipment should be complemented by efforts to innovate and prepare for new risks and threats.

Keywords: COVID-19 pandemic; cooperation; defence capabilities; equipment programmes; military expenditure;

INTRODUCTION

In 2008-2009, the security environment was still under the influence of classical risks and threats, such as terrorism, the proliferation of mass destruction weapons, inter-ethnic conflicts, or organised crime. In addition, the economic and financial crisis triggered not only economic but also political and social effects, with strong implications for military budgets. States and regional and international organisations had to adjust their defence planning and to find new cooperation strategies in order to reduce spending and, at the same time, strengthen their armed forces.

The former High Representative of the European Union for Foreign and Security Affairs, Catherine Ashton, stated, in May 2011, that the European Union aimed to turn the financial crisis and its impact on national defence budgets into an opportunity to increase cooperation in terms of developing military capabilities. Thus, pooling and sharing the resources, prioritising, specialising and finding multinational solutions have become central points in defining new defence strategies.

Through the Pooling and Sharing initiative, the European Union aimed to ensure the continuation of the process of developing military capabilities, in the context of the global economic and financial crisis. Cost-effectiveness required the coordination and harmonisation of military requirements between member states, as well as the assessment of financial priorities for the development and acquisition of new military capabilities. Moreover, in order to increase the effectiveness of these activities, the duplication of capabilities had to be avoided, both within the European Union and within NATO-EU strategic partnership. The implementation of this cooperation initiative was not a singular action, NATO member states adopting a measure with a similar goal, the Smart Defence initiative. The two concepts, imposed by cost efficiency needs, have become representative in the defence sector, with cooperation turning into a significant feature in the reconfiguration of new security strategies.

After more than ten years since the financial crisis and budgetary constraints affected the defence acquisitions programmes, we are once again in front of a new potential crisis, generated by the COVID-19 pandemic and the effects that the drastic measures adopted during this period have had on the economic growth. Thus, the purpose of this article is to present the perspectives of the European defence institutions on cooperation projects between states in the context of the pandemic. We aim to analyse the efforts taken, both at national and regional level, in relation to the challenges posed by the pandemic and its consequences on public health and the social and economic security of citizens, as well as the positions of European Union representatives on the impact that the COVID-19 has on the efficiency of the armed forces.

EXAMPLES OF ACTIONS TAKEN BY THE ARMED FORCES DURING THE PANDEMIC PERIOD

We have noticed, since the beginning of 2020, that military personnel have been among the first institutions to respond constructively to the coronavirus pandemic, being early mobilised for various actions such as building hospitals, distributing medicines and protective materials and necessary goods to the isolated or quarantined persons, but also in the repatriation or evacuation missions.

In *Italy*, one of the European countries most affected by the pandemic, the armed forces have been mobilised from the beginning to help enforce quarantine and maintain the security level. These activities were part of the *"Strade Sicure" operation (Operatione Strade)*. The armed forces have taken action in order to build field hospitals, transport patients, disinfect and sanitise public spaces, distribute medical products and provide specialised personnel. At the request of the Department of Civil Protection, in order to adequately deal with the emergency caused by the pandemic, the armed forces provided aircraft, ground vehicles and the necessary infrastructure to accelerate the distribution of personal and necessary protective equipment in the fight against the virus. Considering that fast responses were necessary to ensure an efficient distribution of medical and protection products, the Italian armed forces involved the Logistic Regiment of the Mechanised Brigade *"Pinerolo"* in the areas most affected by the virus, a logistics unit having a high capacity of materials handling (Ibid.). The Viterbo Air Force, which is a central unit for rescue operations, had the mission of administering and manoeuvring the bio-isolation stretchers *"IsoArk N36"* and mobilising several regiments, prepared to intervene in emergency situations (Esercito, 2004). The 3rd Air Support Regiment *"Aquila"* was also engaged in the Bergamo region in handling the effects of the high incidence of mortality, in collaboration with the civilian authorities and with logistical assistance and specialised personnel provided by the Russian Federation (Ibid.).

In France, in March 2020, President Emmanuel Macron launched a resilience operation *("Opération Résilience")* (Macron, 2020) in the fight against the coronavirus pandemic. This plan involved effective mobilisation consisting of logistical assistance for the health sector. The French Naval Forces carried out evacuation missions and mobilised the Tonnerre amphibious assault helicopter carrier and 200 sailors in order to support the civilian forces on the island of Corsica. The Air Force contributed to the evacuation, transport of patients and repatriation of French citizens from China. The National Agency for the Security of Information Systems was also mobilised to combat phenomena such as fake-news or attacks on strategic technological systems and communication networks (Assemblée Nationale, 2020). The resilience operation aimed to coordinate the actions of the French armed foces in three main areas: sanitation (by putting into operation field hospitals and carrying out decongestion operations in the most affected areas), logistics (by air, sea and ground transport of patients and health and protection materials, as well as by providing expertise and professionals), protection (support in the surveillance of sensitive areas, along with internal security forces) (Ibid.). Tests and performance measurements for several prototypes of protective masks have also been achieved within the Directorate-General for Armaments.

In *Germany*, the air force contributed to the repatriation of citizens, to the distribution of food, medicine and field beds. They also achieved patient transfer missions, both in Germany and from France and Italy. The land forces set up field hospitals, provided medical support and mobilised about 2,000 volunteer reservists in medical actions. The naval forces also took part in actions to help the citizens. In addition, as part of the support provided during this period, the armed forces procurement office allocated 241 million euros for the purchase of protective medical equipment (German Ministry of Defence, 2020).

Spain is another example of a state that has faced a very large number of cases of COVID-19. The military forces played a very important role in managing the situation imposed by the adoption of harsh restrictions. At the beginning of the pandemic, in March, the Spanish Ministry of Defence implemented the military operation *"Balmis"*. Thus, soldiers from the Military Emergency Unit were mobilised to implement activities of inspection and disinfection in public spaces. The transmission battalion of the same unit received two drones from a private company for their adaptation and use in the process of disinfection of large areas. For the same purpose, the Ministry of Defence took the initiative to develop a germicidal irradiation device with ultraviolet light. The air and land forces also provided logistical support in transporting patients and distributing medical equipment, as well as setting up field hospitals in several affected regions. The Spanish armed forces continue to be mobilised throughout the year to help maintain quarantine and slow the spread of the virus, by creating a tracking system for early detection of infection, and establishing epidemiological surveillance units (Spanish Ministry of Defence, 2020).

In Romania, the Ministry of National Defence deployed the armed forces from the beginning of the pandemic, for the installation of epidemiological triage tents. Specialists in several fields (medical, procurement and logistics) provided support to local and central authorities. According to military ordinance number 3/2020, at the request of the Ministry of Internal Affairs, the army intervened in public order missions and provided personnel and logistical means to support the activities of the Romanian Border Police. Moreover, the Ministry of National Defence installed the ROL 2 medical team, implemented missions for the transport and distribution of approximately 45 tons of medical equipment from Seoul to Bucharest and 21 tons of protective materials from Turkey (Romanian Ministry of Defence). Through the NATO Support and Procurement Organisation – NSPO, the Ministry of National Defence purchased 200 tons of medical materials and equipment, worth 15 million euros (Ibid.).

In addition to the missions of logistical support, procurement and support in building hospitals or coordinating medical activities where necessary, the Ministry of National Defence also contributed to the design and development of equipment to support hospitals and authorities in Romania in the fight against the COVID-19 pandemic. Researchers and military doctors from the Military Equipment and Technologies Research Agency and the Military Medical Research Centre developed the first type of isolation stretcher of Romanian design and production; a medical mechanic ventilator was also designed within *"Ferdinand I"* Military Technical Academy (Ibid.). The Ministry of National Defence also undertook missions to provide support with equipment and medical personnel to the states severely affected by the spread of the virus: Spain, Italy, the Republic of Moldova, the USA.

The above-mentioned examples demonstrate that military personnel were among the first institutions to respond to the challenges of the pandemic. Despite the fact that the defence budgets have been reduced in the recent years as a result of the economic crisis of 2008-2009, the armed forces of the European states have been mobilized since the beginning of this period and have provided support in the transport and distribution of medical equipment, protection, construction of field hospitals, repatriation and evacuation of citizens, maintenance of public order, disinfection actions, resources provision and specialised personnel for the medical and research sector.

The military forces' responses to the health crisis were discussed in April 2020, during a video conference chaired by Josep Borrell, the High Representative of the European Union for Foreign Affairs and Security Policy. Defence ministers discussed the impact of the pandemic on defence and outlined the efforts made in the fight against the virus and the status of the missions and operations under the Common Security and Defence Policy (Defence Ministers videoconference, 2020). In this context, the EU Defence Ministers decided to create a dedicated task force at the level of the EU Military Staff, with the aim of sharing information and expertise between member states on the military assistance in support of civilian authorities. This working group would strengthen strategic communication efforts and help identify lessons and practices that can be used in the future. General Claudio Graziano, President of the EU Military Committee, confirmed the involvement of all defence ministers of the member states, arguing that sharing expertise and increasing the capability of European armed forces will become a priority, reflected in future EU defence initiatives (Lațici, 2020).

THE ECONOMIC IMPLICATIONS OF THE COVID-19 PANDEMIC AND THE EUROPEAN INSTITUTIONS APPROACH TO COOPERATION INITIATIVES

The International Monetary Fund predicts a slowdown of the economic growth by 4.9% globally, due to the negative impact that the COVID-19 pandemic had on the economic activity in the first half of 2020. A new economic shock is expected and, most likely, the defence budgets, which are unlikely to recover from the 2008-2009 financial crisis, will once again be subject to adjustments. Defence and integration initiatives, such as PESCO (Permanent Structured Cooperation) or the European Defence Fund, are dependent on financial contributions from states, and if they are affected by a new economic crisis, then the resources for common defence projects will be also reduced. In addition, the restriction of activities during the pandemic will have consequences for the defence industry, such as blocking supply and distribution chains, delaying delivery for military products, as well as the research, development and innovation projects for defence (Ibid.). The negative effects of a possible financial crisis on military expenditure will not only be felt at the national level, but will also affect the projects and programmes that the European Union is trying to implement in the security and defence sector. The awareness of the risks posed by lower spending and the reorientation of the military equipment efforts at national level should drive the EU to maintain the solidarity and to strengthen the cooperation policies and strategies.

In 2018, the European Commission proposed the allocation of 13 billion euro to the European Defence Fund, in order to facilitate the process of cooperation between companies and between EU member states in research and development projects for defence (Internal Market). However, the forecast of the economic situation for the coming years will prevent the achievement of many such objectives. The EU's long-term budget for 2021-2027 was adopted under the economic and social pressures from the pandemic, with most of the negotiated agreements being conducted to the Union's recovery after the quarantine period in the first part of the year. Thus, the perspective on defence cooperation projects has changed. The European Defence Fund received a budget of 205 million euros (European Defence Fund, 2020). These funds will be directed to the development of capabilities such as: military drones and related technologies, space technologies, UGV (unmanned ground vehicle) solutions, high precision missile systems, future naval platforms, airborne electronic attack capabilities, tactical and highly secured networks, cyber situational awareness platforms, or next generation of active stealth technologies (Ibid.).

Although we cannot yet quantify the effects of the pandemic on economic growth and we cannot anticipate when a new financial crisis will break out, this above-presented example of a defence budget cut reflects the inconsistency on the European defence strategy. In this context, the strengthening of military cooperation initiatives remains an indispensable factor in the security and defence policies of the European Union.

Presumed budget cuts will affect the ability of some member states to initiate or continue national equipment and development programmes and the consequences will be felt within the European Union's defence strategy as well. This fact could, however, intensify the defence cooperation process. According to Jiří Šedivý, Executive Director of the European Defence Agency, Europe needs more than ever a consolidated joint defence and capability planning (Europe Defence Matters, 2020). The development, planning, procurement, operation and support of the equipment at multinational level, either under the auspices of PESCO or the European Defence Agency, is more cost-effective and interoperable and could have a greater impact comparing to the isolated efforts taken by the states at national level.

Tomislav Ivić, the Secretary of State for Defence in Croatia, who held the Presidency of the European Union in the first part of 2020, considers that the necessary steps to strengthen the cooperation efforts are: ensuring coherence in initiatives by integrating the European defence capabilities into the national strategies of planning, the cooperation at EU level, helping and advising the member states in the process of identifying capabilities and technologies that can be jointly developed, and the cooperation with strategic partners (Ibid.). It is also important to strengthen the initiatives of PESCO and the European Defence Fund, which are guided by principles such as cooperation and sharing of common values and interests. Understanding the new types of threats, adapting or developing new response mechanisms and the innovation of the security technologies should be a permanent task of the European Union, which assumes the role of security guarantor in the region. One of the lessons learned from the current pandemic is the importance of the response time and the efficiency of cross-sectorial coordination. Thus, we consider that the way in which national and European institutions approach the process of cooperation between various actors, from governments, research institutions, defence industry, private sector, to the military, civil society and citizens is a key element in achieving these goals.

CONCLUSIONS

The armed forces have provided support to civilian authorities in various sectors since the beginning of the COVID-19 pandemic, from the construction of hospitals, to the provision of medical personnel and equipment, transportation, procurement and logistical activities. This has been reflected at both national and multinational level. There have been many criticisms of the European Union's delayed response to this global crisis. However, the national armed forces have also been deployed to support missions in other states most severely affected by the pandemic, and this mobilisation is one of the visible methods of cooperation, as a response mechanism to an unprecedented crisis. We conclude, therefore, that the role of the defence capabilities must represent the focus of attention of decision-makers in the military sector. The actions taken during this period and briefly analysed at the beginning of this article show that the tasks of this sector are indispensable in addressing not only classical threats, but also new types of challenges. The COVID-19 pandemic is an opportunity to identify and prioritise capabilities that can be improved or developed in order to deal with similar situations in the future. Therefore, defence budgets must be treated responsibly and cooperation and coordination efforts must be constantly strengthened.

BIBLIOGRAPHY:

1. Csernatoni, R. (2020). *"EU Security and Defence Challenges: Toward a European Defence Winter?"*. Carnegie Europe, https://carnegieeurope.eu/2020/06/11/eu-security-and-defense-challenges-toward-european-defense-winter-pub-82032, retrieved on 16 September 2020.
2. Lațici, T. (2020). *"The role of armed forces in the fight against coronavirus"*. EPRS (European Parliamentary Research Service), https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/649401/EPRS_BRI (2020)649401_EN.pdf, retrieved on 3 August 2020.
3. European Commission, https://ec.europa.eu/, retrieved on 12 September 2020.
4. Consilium Europa, https://www.consilium.europa.eu, retrieved on 2 August 2020.
5. European Defence Fund (2020). Brussels, https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1053, retrieved on 6 April 2020.
6. Europe Defence Matters. European Defence Agency (2020), https://eda.europa.eu/docs/default-source/eda-magazine/edm19_web.pdf, retrieved on 3 August 2020.
7. Internal Market, https://ec.europa.eu/growth/sectors/defence/european-defence-fund_en, retrieved on 29 September 2020.
8. French Ministry of Defence, https://www.defense.gouv.fr/, retrieved on 23 September 2020.
9. German Ministry of Defence, https://www.bmvg.de, retrieved on 23 September 2020.
10. Italian Ministry of Defence, http://www.esercito.difesa.it, retrieved on 23 September 2020.
11. Romanian Ministry of Defence, https://www.mapn.ro, retrieved on 23 September 2020.
12. Spanish Ministry of Defence, https://www.defensa.gob.es, retrieved on 23 September 2020.
13. *„Opération Résilience"*. Emmanuel Macron Speech, 25 March 2020, https://www.elysee.fr/emmanuel-macron/2020/03/25/a-mulhouse-aux-cotes-des-femmes-et-des-hommes-mobilises-en-premiere-ligne-pour-proteger-les-francais-du-covid-19, retrieved on 28 September 2020.
14. European Parliament, https://www.europarl.europa.eu, retrieved on 23 September 2020.
15. Rapport d'Information. Assemblée Nationale (2020), http://www.assemblee-nationale.fr/dyn/15/rapports/cion_def/l15b3088_rapport-information, retrieved on 12 September 2020.
16. Defence Ministers Videoconference, EU Council, 6 April 2020, https://www.consilium.europa.eu/en/meetings/fac/2020/04/06/, retrieved on 29 September 2020.
17. https://www.elysee.fr/emmanuel-macron/2020/03/25/a-mulhouse-aux-cotes-des-femmes-et-des-hommes-mobilises-en-premiere-ligne-pour-proteger-les-francais-du-covid-19, retrieved on 28 September 2020.
18. http://www.esercito.difesa.it/comunicazione/Pagine/esercito-contro-il-covid-19_200414.aspx, retrieved on 28 September 2020.

19. https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1053, retrieved on 29 September 2020.
20. https://www.lastampa.it/vercelli/2020/03/24/news/coronavirus-nell-operazione-strade-sicure-impegnati-anche-i-militari-dell-esercito-1.38631066, retrieved on 28 September 2020.

RISKS TO NATIONAL SECURITY IN THE CONTEXT OF THE COVID-19 PANDEMIC

Major Carmen Maria IEPURE (MOISE), PhD Student

"Carol I" National Defence University, Bucharest

The COVID-19 pandemic brought with it not only the risk of infection with a new virus but also the possibility of attacks on national security by affecting national critical infrastructure. Maintaining a greater focus on national security is a necessity in any situation.

During this pandemic period, the most affected critical infrastructure sector is health. We hope that the measures taken will lead us to a stabilisation of the situation and not to witness a more pronounced affectation of this sector. We must also pay special attention to the trust in the public administration in order not to be undermined by state or non-state actors with various economic and geostrategic interests on the Romanian territory.

Keywords: risk; pandemic; national security; COVID-19, China;

INTRODUCTION

The end of 2019 brought with it concerns (COVID-19 pandemic) from China, a country where a new type of virus was identified that was spreading quite quickly among the population. It was initially thought that the virus could be controlled to spread to a limited geographical area, but this could not be achieved because the mobility of citizens has increased substantially, with international events facilitating the spread of the new virus.

More and more countries have started to report the existence of the new virus on their territory. The first major shock was felt by the massive spread in Italy (The worst day for Italy), where the sanitary system barely handled the wave of hospitalisations.

The subsequent evolution of infections in various states of the world, led the World Health Organisation (WHO) to declare, on 11.03.2020, that *"the coronavirus epidemic is officially a pandemic"* (Radio Free Europe, 11 March 2020). *"The COVID-19 viral disease that has ravaged at least 114 countries and has killed more than 4,000 people is now officially a pandemic"* the World Health Organisation said on Wednesday. *"This is the first pandemic caused by coronavirus"*, said WHO Director-General Tedros Adhanom Ghebreyesus. Thus, the official name for the new coronavirus is SARS-CoV-2 (severe acute respiratory syndrome coronavirus 2), and the name for the disease it causes is COVID-19 (Ibid.).

ESTIMATION AND MATERIALISATION OF THE RISK OF MASS INFECTION WITH A VIRUS

Once with the official declaration as a pandemic of the epidemic caused by the infection with a new type of coronavirus, now recogniSed by the official name of SARS-CoV-2, from the perspective of risk management we are dealing with the manifestation of a potential risk identified by specialists in various official documents. From this point we are not dealing with an identified potential risk, but with a manifested risk that has become a real problem that needs to be managed.

Strong states with a well-developed risk management that had long planned, in official documents, measures to be taken if there is a risk of mass infection, were taken by surprise and probably based on a well-developed public health system they assumed a higher risk, not taking such harsh and early measures as in the states where the health system is not performing, in this case, we will refer to that of Romania.

In the analysis made for this article we will refer to the UK and the USA.

We started from the analysis of the risk of infection with a virus or other type of pathogen and the measures established for this type of risk included in the national security strategies of the two states.

In the US National Security Strategy of December 2017, at p. 9, we find the potential risk of biological threats and pandemics, as well as the measures proposed to respond to these potential risks.

The measures proposed in the strategy are:

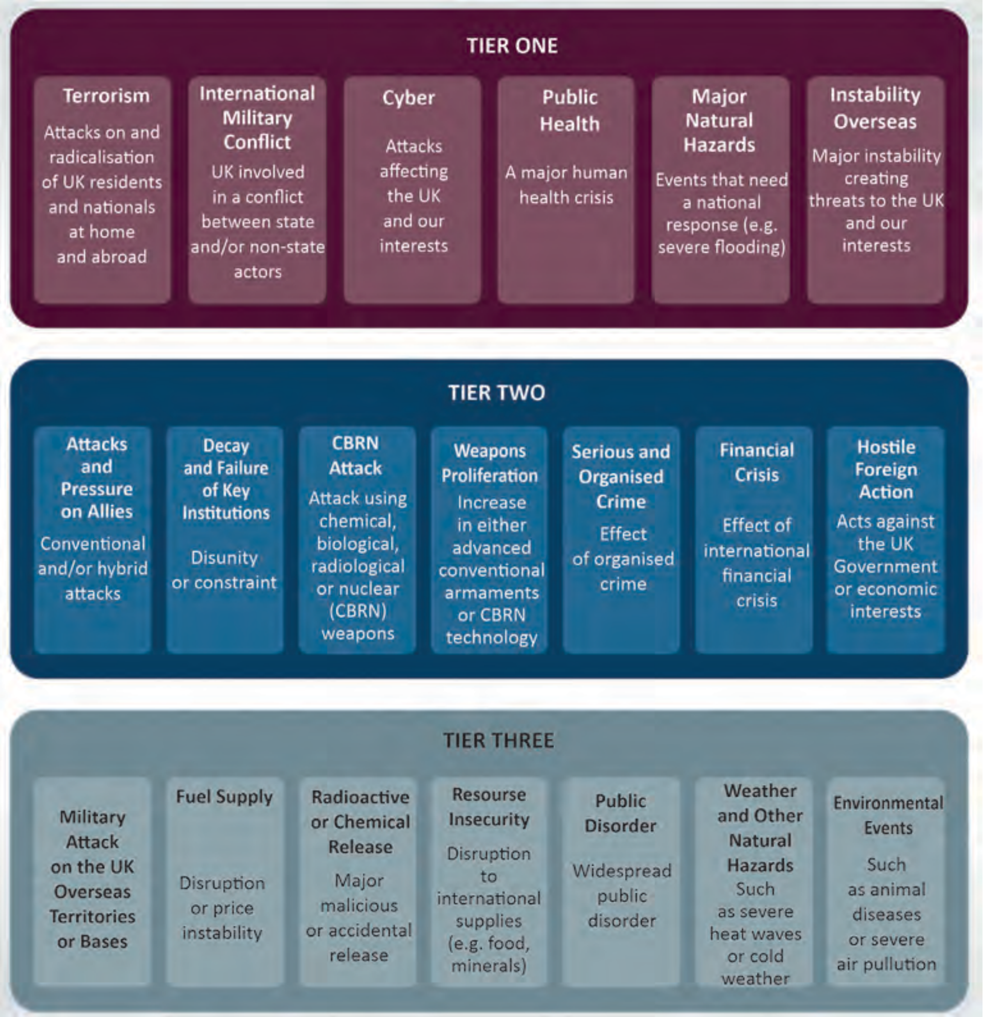
- **detecting and maintaining biological and pandemic threats at their source** by collaborating with other countries to identify outbreaks in a timely manner to prevent the spread of the disease, encouraging other states to invest in health systems to strengthen global health security, ensuring that laboratories in which dangerous pathogens are investigated will benefit from safety and security measures;
- **supporting innovation in biomedicine** by strengthening the intellectual property system in the biomedical industry;
- **improving the emergency response** by implementing measures to limit the spread of disease and providing emergency medical care (Ibid.).

In the National Security and Strategic Defense Strategy of 2015 of the UK, objective no. 1 is the **Protection of our people** and in Annex A is presented a summary of the National Security risk assessment for the next five years, by 2020.

Among the identified risks we find in Public Health, p.86 of the strategy: risks of diseases, especially pandemic influenza, emerging infectious diseases and increased antimicrobial resistance. These are considered threats to life, public health, services and the economy. The United Kingdom is considered vulnerable due to its large population and open society (Ibid.).

Also, as priority no. 1 (Tier one) we find the protection of Public Health, as it can be seen in the image taken from the strategy (*Figure no. 1*).

A detailed presentation of the risks to public health as well as other types of risk can be found in the National Register of Civil Emergency Risks, 2017 Edition (*Figure no. 2*).



TIER ONE

Terrorism	International Military Conflict	Cyber	Public Health	Major Natural Hazards	Instability Overseas
Attacks on and radicalisation of UK residents and nationals at home and abroad	UK involved in a conflict between state and/or non-state actors	Attacks affecting the UK and our interests	A major human health crisis	Events that need a national response (e.g. severe flooding)	Major instability creating threats to the UK and our interests

TIER TWO

Attacks and Pressure on Allies	Decay and Failure of Key Institutions	CBRN Attack	Weapons Proliferation	Serious and Organised Crime	Financial Crisis	Hostile Foreign Action
Conventional and/or hybrid attacks	Disunity or constraint	Attack using chemical, biological, radiological or nuclear (CBRN) weapons	Increase in either advanced conventional armaments or CBRN technology	Effect of organised crime	Effect of international financial crisis	Acts against the UK Government or economic interests

TIER THREE

Military Attack on the UK Overseas Territories or Bases	Fuel Supply	Radioactive or Chemical Release	Resourse Insecurity	Public Disorder	Weather and Other Natural Hazards	Environmental Events
	Disruption or price instability	Major malicious or accidental release	Disruption to international supplies (e.g. food, minerals)	Widespread public disorder	Such as severe heat waves or cold weather	Such as animal diseases or severe air pullution

Figure no. 1: Priorities regarding UK security. (Ibid., p. 87)

Figure no. 3 presents a risk matrix as well as a more detailed presentation of the risks and measures that have been taken in the past and could be taken in the future.

As a potential to cause a civil emergency, diseases are identified that can cause the infection of a large number of people in a short time. Influenza is mentioned as a disease, not the seasonal one, but the flu caused by a new virus that would spread quickly and cause serious diseases due to lack of immunity. It is stated that there is a high probability of occurrence of this kind of pandemic, taking into account the history of such pandemics, but it cannot be accurately estimated when it will occur.

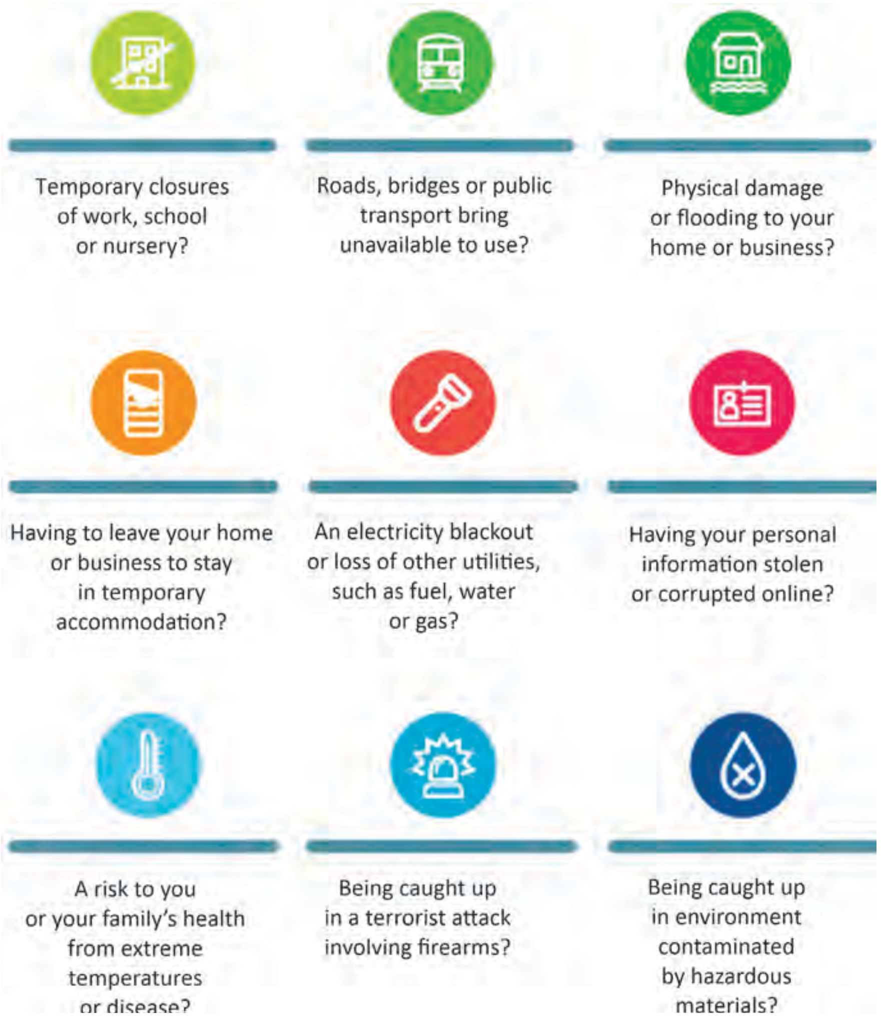

Temporary closures of work, school or nursery?
Roads, bridges or public transport bring unavailable to use?
Physical damage or flooding to your home or business?
Having to leave your home or business to stay in temporary accommodation?
An electricity blackout or loss of other utilities, such as fuel, water or gas?
Having your personal information stolen or corrupted online?
A risk to you or your family's health from extreme temperatures or disease?
Being caught up in a terrorist attack involving firearms?
Being caught up in environment contaminated by hazardous materials?

Figure no. 2: The main types of risks (National Register of Civil Emergency Risks, 2017, p. 12)

There are also estimated the consequences of pandemic flu:

1. If up to 50% of the UK population has symptoms, it is estimated between 20,000 and 750,000 deaths and high levels of absence from work.

2. Disruption of essential services, in particular health and education; and

3. Economic disruptions, including disruptions to business and tourism.

Examples of pandemic outbreaks are mentioned in the register, an H1N1 strain (*"swine flu"*) in 2009, which caused at least 18,500 deaths worldwide (*Figure no. 4*).

In 1918, another variant of the same strain of H1N1 *("Spanish flu")* killed more than 50 million people worldwide. However, there are other pandemic influenza strains, such as H5N1 *("avian or avian influenza")*. This strain caused several hundred human deaths in Southeast Asia in 1996.

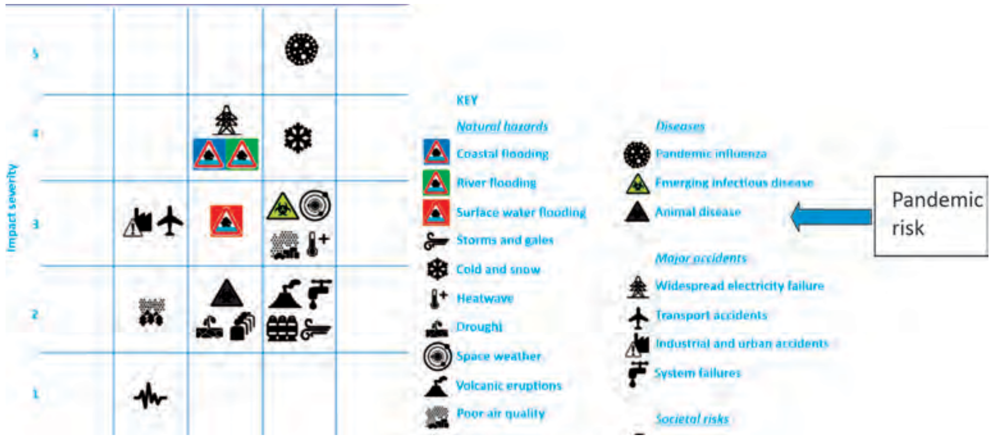


Figure no. 3: Matrix of natural disasters, diseases, accidents and social risks for five years
(National Register of Civil Emergency Risks, p. 9)

It is mentioned that in the last 25 years more than 30 new (or recently recognised) emerging infectious diseases have been identified worldwide, such as Ebola, Zika and respiratory syndrome in the Middle East. The latter emerged recently in 2012 and posed a global threat to health.

Solutions we find in the registry are:

1. Before the manifestation of the risk

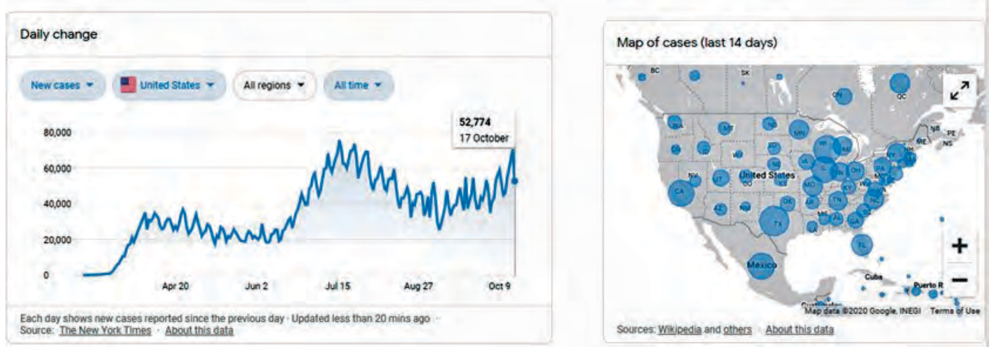
- **Planning** – The UK Pandemic Influenza Preparedness Strategy covers strategic planning, response and scientific evidence. There are many contingency plans for many infectious emerging diseases. The World Health Organisation manages global influenza preparedness plans.
- **Coordination** – Government departments, decentralised administrations, public health agencies and developed branches need to share plans and information.
- **International collaboration** – the UK Government works with others to undertake research on prevention, detection and research. The World Health Organisation has an influenza programme that provides member states with strategic guidance, technical support and coordination of activities.

2. The risk response

- **Disease detection** – there are specialised capabilities in epidemiology and microbiology in the UK to identify, characterise and respond to infectious diseases.

- **Antivirals** – the government stores enough antivirals to help treat people who have symptoms during a flu pandemic. Antivirals can help treat flu symptoms.
- **Vaccines** – vaccines will be developed as soon as possible once new influenza strains are identified. This will take at least four to six months after the onset of a pandemic.
- **Personal protective equipment** – emergency interventions have personal protection with equipment for severe pandemics and infectious diseases. There are also protocols in place to control infections both before and during an incident.

From our research we see that the two governments have assessed this type of risk and have taken action accordingly. However, with the onset of the COVID 19 pandemic, these states have been affected and are having a rather difficult time managing the situation, with the number of cases rising alarmingly from day to day (COVID-19 update at the date of writing the article). (*Figure no. 4* and *Figure no. 5*).



Each day shows new cases reported since the previous day · Updated less than 20 mins ago · Source: The New York Times · About this data

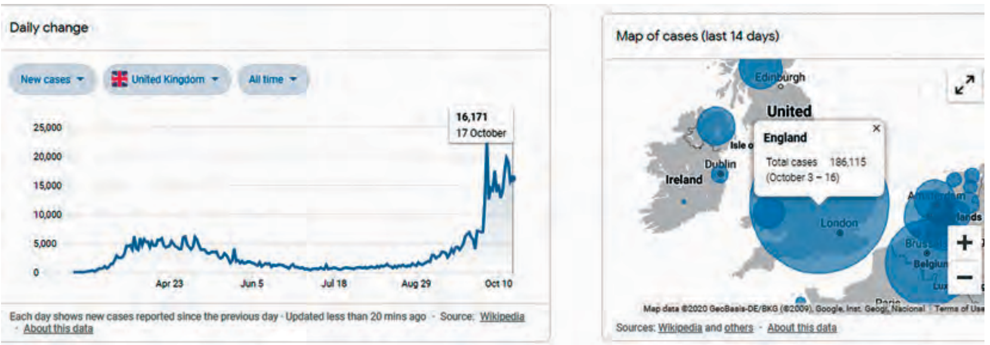
Sources: Wikipedia and others · About this data

Figure no. 4: COVID-19 cases on 17.10.2020, USA (Coronavirus update)

RISKS TO NATIONAL SECURITY IN THE CONTEXT OF THE COVID-19 CRISIS

Focusing on establishing and implementing measures to combat the effects of the pandemic may lead to a diminished focus on security risks.

In a recent interview for Digi24, NATO Deputy Secretary General Mircea Geoană stated that in the context of the COVID-19 crisis, at NATO level, a certain degree of alertness and vigilance is maintained. *"We are, on the one hand, vigilant about the health crisis itself, but especially at the risk of being tempted by state or non-state actors to take advantage of a time when we are all busy – allocating resources, we are concerned with public opinion, the attention of the political and decision-maker naturally goes to this pandemic, the fight against the pandemic, the economic recovery, all that means the range of measures we must take – to take advantage of a vain hope. We discourage, including through public communication actions, to say very clearly that there is no risk to the citizens of the North Atlantic Alliance and we are paid and have an explicit mandate to prevent a major health and economic risk from turning into a security crisis"*.



England
Total cases 186,115
(October 3 – 16)

Each day shows new cases reported since the previous day · Updated less than 20 mins ago · Source: Wikipedia · About this data

Sources: Wikipedia and others · About this data

Figure no. 5: COVID-19 cases on 17.10.2020, United Kingdom (Ibid.)

Security risks are managed through multiple levers, an example being the management of national critical infrastructures. In the US there is a Cybersecurity & Infrastructure Security Agency (CISA), which collaborates with government and industry to identify, analyse, prioritise, and manage the most significant strategic risks to the nation's critical infrastructure (*Figure no. 6*).

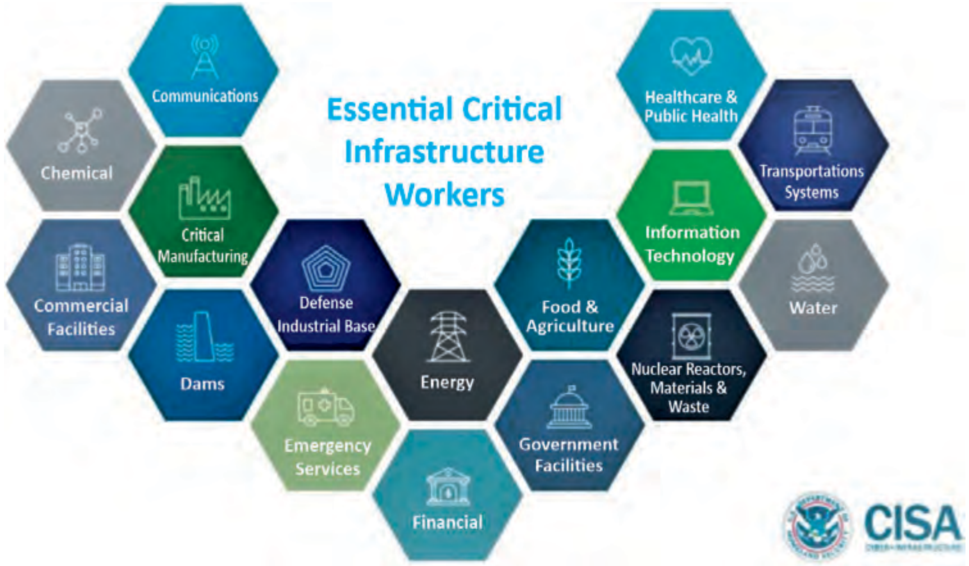


Figure no. 6: US critical infrastructure national sectors (CISA)

The main threats to national security are terrorism, espionage, cyber threats and the proliferation of weapons of mass destruction, many of which have an impact on national infrastructure. They have various hybrid forms of attack, such as: misinformation by fabricating false and manipulative information, data collection applications, cyber attacks etc.

National infrastructure sectors are key strategic interests for foreign intelligence services, whose targeting against sectors is likely to include espionage for economic, political, military or commercial purposes. State agencies, the military and companies working on sensitive technologies are the main targets for foreign espionage.

In the USA, 16 critical infrastructure sectors are identified whose assets, systems and networks, whether physical or virtual, are considered vital to any state. Their incapacitation or destruction would have a direct effect on security, national economic security, public health or national security, or any combination thereof.

They can be identified in any state but they can be more or less developed. Threats of any kind to critical infrastructure are important issues that must be addressed as a matter of priority, as a threat to national security.

In Romania, the critical infrastructures were established by Emergency Ordinance no. 98/2010 on the identification, designation and protection of critical infrastructures, following the implementation of the European Council Directive no. 114/2008 on the identification and the designation of European Critical Infrastructures and the assessment of the need to improve their protection. The preamble to the emergency ordinance mentions an essential element in the link between the maintenance and development of critical infrastructure and national security *"ensuring an adequate level of protection of critical infrastructure is essential for economic development, the maintenance of vital functions of society and the safety of citizens, as well as the fact that failure to adopt such regulation in an emergency could undermine national security"* (Ibid.). This was amended in 2018 by Law no. 225/2018 for the amendment and completion of the Government Emergency Ordinance no. 98/2010 on the identification, designation and protection of critical infrastructures.

According to the national legislation, at the level of Romania, 12 sectors of national critical infrastructure have been established. They are presented in *figure no. 7*.

Not coincidentally, the Romanian Intelligence Service was appointed responsible for authority for the IT&C and national security sectors, together with other institutions. The Ministry of Health and the Ministry of Education, Research, Youth

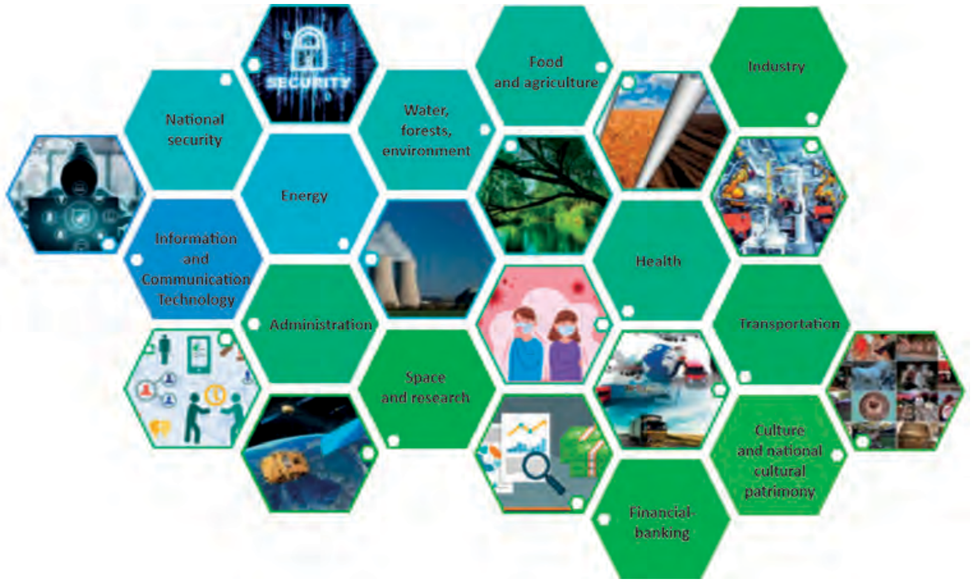


Figure no. 7: Romania's national critical infrastructure sectors

and Sports are responsible for all matters related to public health and research in this critical infrastructure sector according to the law:

"5.1. Medical and hospital care;

5.2. Medicines, serums, vaccines, pharmaceuticals;

5.3. Biolaborators and bioagents;

5.4. Medical emergency services and medical transport". (Ibid.)

Also, according to art. 4. of the law, *"(1) The coordination, at national level, of the activities regarding the identification, designation and protection of ICN / ICE is carried out by the Prime Minister, through the appointed adviser. In order to fulfil the responsibilities established by this emergency ordinance, the Prime Minister issues decisions.*

(2) The responsibility for organising and carrying out the activities necessary to implement the legislation specific to the PIC field rests with the Ministry of Internal Affairs, hereinafter referred to as MAI, through the National Center for Coordination of Critical Infrastructure Protection, hereinafter referred to as CNCPIC" (Ibid.).

One aspect that caught our attention is the fact that in Romania, national security is considered a critical infrastructure sector. From our point of view, taking into account the analysis of critical infrastructures in other states such as the USA (see figure no. 6), Canada – sectors: Energy and Utilities, Finance, Food, Transport, Government, Information and Communication Technology, Health, Water, Manufacturing, Safety (Canada's Critical Infrastructure, May 2020) and Australia

– Banking and Finance, Communications, Data and Cloud, Defence Industry, Education, Research and Innovation, Energy, Food and Agriculture, Health, Space, Transport and Water (Protecting Critical Infrastructure and Systems of National Significance, August 2020), national security covers all sectors of national critical infrastructure and any deficiency in one of the sectors has repercussions on national security.

Based on these aspects, we can deduce that a poor or medium-developed health sector, in the face of a pandemic, faces much more difficulty than a well-developed sector, which can lead to national security by triggering chain reactions: the inability to provide specialised medical care for all sick people, the increase in the number of deaths leading to the loss of human resources, the need to take too harsh measures to limit the spread of the virus (closing restaurants, schools, theaters etc.) which can lead to a unwanted damage to the national economy, to the financial resources of the population, which becomes a threat to the security of the nation – national security.

CONCLUSIONS

In this period of pandemic, unfortunately, we live these measures in Romania and we can only draw the attention of public authorities to the need for a careful analysis of the situation and the maintenance of a level of alert, so as not to endanger national security in the medium and long term.

The most affected critical infrastructure sector today is health. We hope that the measures taken will lead us to a stabilisation of the situation and not to witness a more pronounced affectation of this sector, because it entails the affectation of other sectors as well.

We must also pay special attention to the trust in the public administration in order not to be undermined by state or non-state actors with various economic and geostrategic interests on the Romanian territory.

Risks to national security must be analysed and treated with the utmost care. The risks can be identified most easily, according to the specialists in the field, by formulating cause – risk – effect (Mulcahy, 2010, pp. 70-77).

BIBLIOGRAPHY:

1. Mulcahy, R., *Risk Management, Tricks of the Trade for Project Managers*, PMP, Third Edition, RMC Publications, USA.
2. *Canada's Critical Infrastructure* (19 MQI 2020), https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/cci-iec-en.aspx, retrieved on 29 September 2020.
3. *COVID-19 Update*, https://www.google.com/search?ei=doeMX7HeMeLMrgSsqqPoCg&q=cazuri+covid+sua+azi&oq=cazuri+covid+sua+&gs_lcp=CgZwc3ktYWIQARgA

MgUIABDJA1CngwFYp4MBYKOPAWgAcAB4AIABngGIAbMCkgEDMC4ymAEAoAEBqgEHZ3dzLXdpesABAQ&sclient=psy-ab, retrieved on 13 August 2020.
4. *Cea mai proastă zi pentru Italia: Un nou vârf în bilanțul cazurilor de coronavirus*, https://www.digi24.ro/stiri/externe/ue/cea-mai-proasta-zi-pentru-italia-un-nou-varf-in-bilantul-cazurilor-de-coronavirus-1277646, retrieved on 18 October 2020.
5. *COVID-19 update*, https://news.google.com/covid19/map?hl=ro&mid=%2Fm%2F06c1y&gl=RO&ceid=RO%3Aro, retrieved on 23 September 2020.
6. *Pandemia de coronavirus*, https://ro.wikipedia.org/wiki/Pandemia_de_coronaviroz%C4%83_(COVID-19), retrieved on 18 October 2020.
7. *Protecting Critical Infrastructure and Systems of National Significance*, https://www.homeaffairs.gov.au/reports-and-pubs/files/protecting-critical-infrastructure-systems-consultation-paper.pdf, retrieved on 18 October 2020.
8. Radio Europa Liberă, *Organizația Mondială a Sănătății a declarat oficial pandemie de coronavirus*, https://romania.europalibera.org/a/organiza%C8%9Bia-mondial%C4%83-a-s%C4%83n%C4%83t%C4%83%C8%9Bii-a-declarat-oficial-pandemie-de-coronavirus-%C8%99i-/30482192.html, retrieved on 18 October 2020.
9. https://www.google.com/search?ei=ioeMX5H2KY72qwHjsoaQDg&q=cazuri+covid+anglia+azi&oq=cazuri+covid+Anglia&gs_lcp=CgZwc3ktYWIQARgBMgUIABDJAzICCAA6BggAEBYQHlCqsAxY3r8MYPfRDGgAcAB4AIABqwmIAcQekgENMC4yLjEuNS0yLjEuMZgBAKABAaoBB2d3cy13aXrAAQE&sclient=psy-ab, retrieved on 13 September 2020.
10. https://www.npr.org/sections/goatsandsoda/2020/03/11/814474930/coronavirus-covid-19-is-now-officially-a-pandemic-who-says?t=1603030093740, retrieved on 18 October 2020.
11. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf, retrieved on 19 October 2020.
12. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/478936/52309_Cm_9161_NSS_SD_Review_PRINT_only.pdf, retrieved on 19 October 2020.
13. https://www.gov.uk/government/publications/national-risk-register-of-civil-emergencies-2017-edition, retrieved on 18 October 2020.
14. https://www.google.com/search?ei=doeMX7HeMeLMrgSsqqPoCg&q=cazuri+covid+sua+azi&oq=cazuri+covid+sua+&gs_lcp=CgZwc3ktYWIQARgAMgUIABDJA1CngwFYp4MBYKOPAWgAcAB4AIABngGIAbMCkgEDMC4ymAEAoAEBqgEHZ3dzLXdpesABAQ&sclient=psy-ab, retrieved on 19 October 2020.
15. https://www.digi24.ro/stiri/externe/mircea-geoana-despre-autostrada-romania-polonia-e-un-proiect-de-colaborare-in-cadrul-initiativei-celor-3-mari-si-germania-participa-1385375, retrieved on 19 October 2020.
16. https://www.cisa.gov/coronavirus, retrieved on 19 October 2020.
17. https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32008L0114, retrieved on 20 October 2020.
18. https://lege5.ro/Gratuit/geztqmzxhe/ordonanta-de-urgenta-nr-98-2010-privind-identificarea-desemnarea-si-protectia-infrastructurilor-critice, retrieved on 20 October 2020.
19. https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/cci-iec-en.aspx, retrieved on 20 October 2020.

CONSIDERATIONS REGARDING THE ROLE OF HUMAN RESOURCES IN ENSURING NATIONAL SECURITY

Elena-Alexandra MAZILU (ALEXANDRESCU)

Communications and Informatics Command, Ministry of National Defence

Colonel (r.) Prof. Mircea-Dănuţ CHIRIAC

“Hyperion” University, Bucharest

A considerable contribution to ensuring national security goes to the military system. Within this system, more than ever, the human resources management represents an essential field, with deep implications, we can say determining in ensuring and guaranteeing the security state of our country.

According to the continuous process of change, like in all the domains, also in the military domain it is necessary to develop new strategies, especially in the recruiting and training areas, because these two areas are very important in building a solid and professional team, a strong human resources system which contributes to achieving the strategic goals of national security.

Regardless of the level of military equipment, the quality of human resources remains an essential factor in the process of training and the efficiency of military action.

Keywords: human resources management; security; recruitment; training; team; professionalism;

INTRODUCTION. THE EUROPEAN SECURITY STRATEGY

For fifty years, the European Union has had as its main objective to ensure the defence, freedom and security of the people. Initially, in December 2003, the European Union adopted the European Security Strategy, which refers to the external dimension of Europe’s security. In February 2010, during the Spanish six-month presidency, the Council completed it by adopting the internal security strategy. This strategy was approved by the European Council on 25 and 26 March 2010.

Presently, a new European strategy was established for a security union in the period 2020-2025, focusing on the main areas in which the European Union can contribute to supporting the member states in strengthening the security of all those living in Europe.

This strategy is structured on four main directions of action:

- A future-oriented security environment by intensifying the measures of ensuring physical protection in public spaces, by increasing cyber security against cyber attacks;
- Combating the constantly evolving threats by reanalysing the measures of combating identity theft and online sexual abuse of children;
- Protecting Europeans against terrorism and organised crime by strengthening border security legislation, establishing new action plans regarding firearms trafficking, human trafficking and drugs;
- A strong European security ecosystem.

It is constantly wanted to improve or update the visions, values and objectives that underlie the security of the European Union, in relation to the main risks that Europe currently faces. Among the most important threats to Europe’s security there are terrorism, organised crime, cybercrime, cyber attacks, trafficking in human beings, drug trafficking, economic crime and corruption. Europe wants to develop at the level of each EU member state a security model based on the principles and values of the Union: respect for human rights and fundamental freedoms, the rule of law, democracy, dialogue, tolerance, transparency and solidarity.

This can be achieved by developing a national strategy at the level of each country, the main goal being to prevent crime, to increase the capacity to respond as quickly as possible to natural and man-made disasters, by developing a ppropriate tools.

National Defence Strategy for 2020-2024 *"Together for a secure and prosperous Romania in a world marked by new challenges"*

Romania aligned itself with this objective of the European Union and initially developed the *National Defence Strategy for the period 2015-2019 "A strong Romania within Europe and the world"*, later developing the new *National Defence Strategy for the period 2020-2024 "Together, for a secure and prosperous Romania in a world marked by new challenges"*. The new strategy aims to establish the main directions that Romania is important to follow both internally and externally, so as to ensure the security and prosperity of citizens, to establish the national security interests and objectives, the main threats, risks and vulnerabilities, but also the measures which should be established at the level of the institutions involved, in order to defend and protect against those threats:

"The National Defence Strategy for 2020-2024 "Together for a secure and prosperous Romania in a world marked by new challenges" provides answers to essential questions regarding our priority national objectives for ensuring the security of Romania and its citizens and shows what we have to do in order to achieve them. Public policies in the field of national security will be designed and implemented with the citizen as final beneficiary, in compliance with the national security and defence policy, the strategy will guide the activity of all public institutions with responsibilities in security and defence field" (2020, p. 4).

At the same time, the new strategy emphasises the importance of creating strong armed forces in order to have international and strategic credibility. This can be achieved by ensuring an efficient and performance human resources management, focusing on the professional development of the employees and on the recruitment of qualified employees.

An important aspect that affects all states is the pandemic that triggered an economic crisis that will surely impact the field of defence and, implicitly, human resources management within the Ministry of National Defence. COVID-19 pandemic is a challenge for all mankind, perhaps the greatest challenge to humanity since the end of the Second World War. The way Romania will react to the effects caused by this pandemic will be based on the defining principles of the North Atlantic Alliance: unity, cooperation and mutual support. The security environment in the region and globally remains unchanged, but after this critical period we may face changes in the way some states will understand national security. This is the reason why it is essential, as a member state of the strongest politico-military alliance in the world, to understand quickly those changes, to adapt constantly, to inform ourselves at the highest standards and to continue the procurement and modernisation of the military equipment in the Romanian Armed Forces.

Externally, the strategy assumes its responsibilities as a member of the European Union, NATO, OSCE, UN from a European, Euro-Atlantic and international perspective. *"Romania is building its security strategy based on the premise that its main guarantees are NATO membership and a privileged relationship with the United States of America, a partner that shares its perception about the level of threats in the area of the Alliance's eastern border"* (Ibid., p. 9).

The Defence Policy Objectives for the Period 2020-2023

The strategic objective of the defence policy for the period 2020-2023 is the modernisation and adaptation of the Romania Armed Forces to the risks and challenges specific to the current geopolitical context, as well as the consolidation of Romania's relevant strategic partner profile at NATO, EU level and within the strategic partnership with the USA. The development of military capabilities will be achieved gradually, with an emphasis on the critical ones, configured for both national and collective defence. Such critical capabilities will target robust command and control capabilities, intelligence, surveillance and reconnaissance capabilities, based on developments at NATO level on this dimension to ensure the early warning segment; capabilities to counteract A2AD systems.

It will also aim to develop a strategy for quickly responding and counteracting hybrid threats, which should include elements of strategic communication, securing the information space and increasing the resilience of communications infrastructures to cyber attacks, at the same time with the adaptation of the laws with incidence on the national security to the new threats of hybrid and conventional high technological type.

An important role will be played by the modernisation of military education so that the personnel of the Romania Armed Forces to be prepared not only for classical threats, but also for new technologies and new types of challenges to national security. Another objective considered by the Ministry of National Defence for the reference period is to increase the quality of life of military and civilian personnel by providing housing facilities, as well as providing medical assistance to armed forces personnel and military personnel in reserve and in retirement (Document-sinteză, 2020).

Human Resource Management

Human resource management has a very important role within an organisation or institution and includes several activities, but it can also have an extremely strategic component, which means that it is involved in the overall organisational performance. Human resource management can also refer to issues related to organisational development, health, safety and staff motivation.

The main activities carried out by human resources specialists:

- *Planning human resources* – through organisational design, respectively ensuring the necessary resources for carrying out activities in good conditions and grouping them effectively to facilitate cooperation, communication and decision-making required for all necessary activities, through the design of positions and the development of job descriptions.
- *Recruitment and selection of human resources* – attracting and selecting the most suitable candidates are two essential factors for achieving success at team and organisational level and this process is a constant challenge for Human Resources specialists. The foundation of a company is made up of its people. Their personality, expertise and attitude form a unique mix. As in building a house, choosing the right people will be the pillars of resistance.

The labour market, the economic situation or the appearance of competitors are dynamic factors that can unpredictably influence the situation of a business. That is why the foundation formed by the right employees contributes to maintaining a stable environment in a situation of imbalance of the labour market.

At the end of the second decade of the 21st century, the attitude of potential candidates towards employers has changed a lot. Potential candidates have realised that they have many rights and opportunities, becoming selective as well, without being satisfied with any job offer. At the same time, in recent years the legislation has changed a lot in favour of employees. There are many situations in which an employee is willing to accept interviews just to test the market, take part in several meetings at the same time, choosing from multiple offers, refusing others. Therefore, the public image of a company is very valuable in a recruitment strategy, because even the strategy itself will talk about the organisational culture of that business.

Thus, choosing an efficient and innovative recruitment strategy is a determining factor for many companies. Potential employees analyse a lot the environment and the techniques chosen by employers to promote their ads or approach their candidates.

- *Performance management* has implications in the career plan, in the management of promotions and career and obviously in the area of compensations and benefits. It is carried out mainly through a very well-developed system for evaluating professional performance.

The development of human resources consists in training and improving employees, in supporting them to develop key competencies that will give them the opportunity to excel in accomplishing tasks and responsibilities.

- Rewards management is the process of developing and implementing reward policies and systems. It consists of designing, implementing and maintaining reward systems so that there is a balance between performance and rewards.

Relating to the current context the whole of humanity is experiencing, corroborated with the objectives of the National Defence Strategy for 2020-2024 *“Together for a secure and prosperous Romania in a world marked by new challenges”* we consider that human resources management has an important role in ensuring national security by establishing clear policies and procedures in several directions, namely:

- policies to ensure the safety and well-being of employees;
- applying an approach in which people come first;
- employees face work-related fears, health hazards, and the evolution of the global economy in general;
- it is essential to anticipate and prepare for what is to come, no matter how difficult it may be for us, not just to react to what is happening to us now;
- during this period, we are all affected, both companies and people; I believe that flexibility, organisational culture, adaptability and values are now being checked;
- to contribute to the development of the defence system because it has an essential role in ensuring national security.

- *Career management*

Career is an important aspect and a significant part of the life of an individual as well as a constant struggle to achieve personal goals or objectives. Individuals are eager to develop careers that take into account both personal and family needs and the quality of their life.

According to literature (Klatt, Murdick, Schuster, 1985, p. 380), the concept of career has several meanings.

Career = promotion. This career vision usually involves mobility, promotion in an organisation or in the professional hierarchy.

Career = profession. According to this view, certain occupations constitute a career (managers, professionals, military), while other occupations are thought of as *“positions”* (waiters, unskilled workers or salesmen).

Career = the succession of positions throughout life. In this vision, career represents history.

Other authors (Mathis, Nica, Rusu, 1997, p.135) understand by career the succession of positions, in the ascending order of prestige, through which the employee passes in an orderly manner, according to a predictable rule. Moreover, Gary Johns, in his reference work *"Organisational Behaviour"*, presents career as *"an evolutionary succession of activities and professional positions that a person achieves, as well as the attitudes, knowledge and associated skills that develop from over time"*.

Career management is the process of designing and implementing goals, strategies and plans that could allow the organisation to satisfy your human resource needs, and individuals to meet their career goals (Klatt et al., Ibid.).

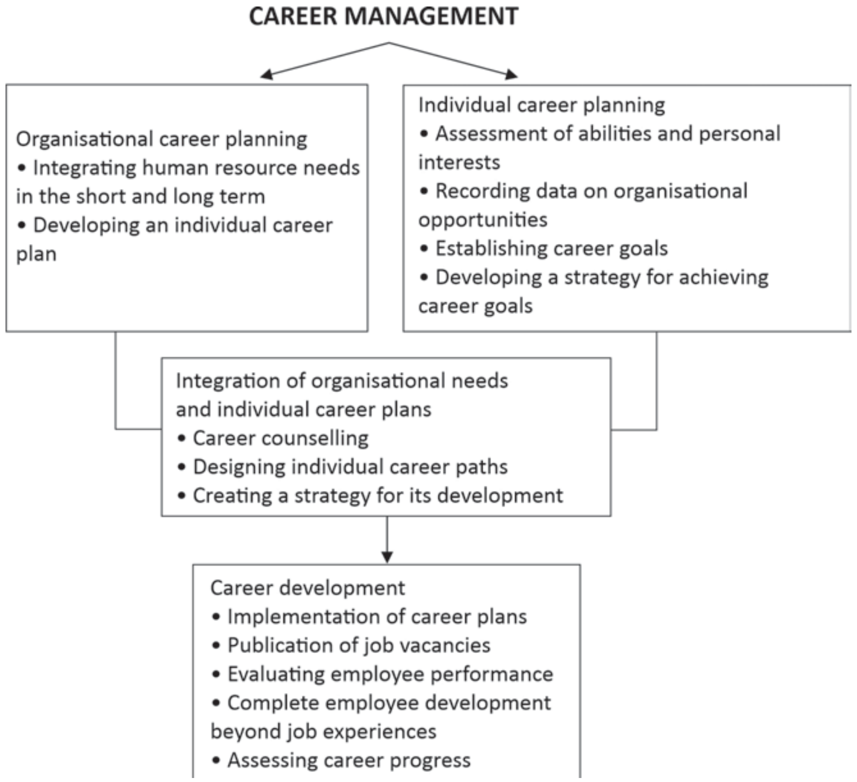

CAREER MANAGEMENT
Organisational career planning
• Integrating human resource needs in the short and long term
• Developing an individual career plan
Individual career planning
• Assessment of abilities and personal interests
• Recording data on organisational opportunities
• Establishing career goals
• Developing a strategy for achieving career goals
Integration of organisational needs and individual career plans
• Career counselling
• Designing individual career paths
• Creating a strategy for its development
Career development
• Implementation of career plans
• Publication of job vacancies
• Evaluating employee performance
• Complete employee development beyond job experiences
• Assessing career progress

Figure no. 1: Career management model (Klatt, Ibid.)

Career management plans and models the progress of individuals within an organisation in accordance with the organisational needs' assessments, as well as their performance, potential and individual preferences (Armstrong, 1991, p. 471). Moreover, career management has multiple links with other human resource management activities. For example, career planning is an integral part of human resource planning, and performance appraisal is one of the necessary conditions for professional career development. From this perspective, human resources planning considers not so much the forecast of vacancies, but the identification of the potential, of the conditions and qualifications required to fill that positions, and performance appraisal is done not so much for substantiating remuneration decisions, but for identifying the development needs of employees. In this context, the international dimension of career management regarding planning and career development of those employees who are going to work abroad should not be neglected either.

In relation to career management, it should also be mentioned that within an organisation, there can be many potential problems (Torrington, Hall, 1995, p. 436), such as:

- if an employee with proper training is proposed several times for promotion, but each time he is rejected or the direct boss does not respond to requests, the employee begins to believe that he has reached an end point in his career or that he is at a point in his career in which the possibilities for promotion are very low;
- promoting an employee to a higher position that does not correspond to his qualification or experience may have undesirable effects, as it is possible that the employee considers that there is no logic in the promotion and that the only solution is to leave the organisation;
- although there are no immediate possibilities to promote an employee and the desire to transfer him to another position is not satisfied, because the direct boss considers that the certain possibilities or qualities of the respective employee are used properly in the existing position;
- although they have real chances for promotion, some employees, bored and frustrated, give up trying to achieve such goals or to realise their own potential.

All of these potential aspects or issues of career management illustrate, in fact, the lack of attention or weak concern of organisations regarding career planning and development.

The potentiated issues mentioned are also only some of the aspects that reflect an inadequate career management that may suggest:

- inadequate feedback regarding career development opportunities;
- low concern for staff promotion;
- avoidance of justified transfers;
- prolonged maintenance on existing positions of well-qualified employees without encouraging their development;
- lack of support for those employees who are not known to have the potential to be promoted;
- the existence of low concerns about employee development opportunities.

The role of human resources management in the development of the defense system:

- establishing special training techniques, improvement by establishing the career plan, by modernising the system of professional training of military personnel, of the military education system;

- development of the selection and recruitment system within the Ministry of National Defence;
- active participation in as many cyber security events, trainings, military missions and exercises as possible;
- allocation of funds/budgets for the development of career management and reward management.

The human resources management process within the Ministry of National Defence is coordinated by the Human Resources Management General Directorate, which promotes an efficient human resources management, focused on professional skills.

Based on the changes appeared during the last years, taking into account the massive volume of retirement requests, but also because of the difficult retention of staff in this field, the main objective of the Human Resources Management General Directorate was to promote military career in civilian environments and to modernise the selection and recruitment process.

The Ministry of National Defence aims to develop on the Romanian labour market, to be a brand recognised under the name of *"Romanian Armed Forces"*, which is a strong institution, which makes those who work there proud (Human Resources Management General Directorate, 2018, p. 7).

Furthermore, the Ministry of National Defence also intends to develop a modern career management focused on identifying the operational requirements of the armed forces, contributing to the compatibility of the human resources management activities of the Romanian armed forces with those of the armed forces of the other member states of the North Atlantic Alliance.

Through the specialists within the Personnel Management Office, military personnel are informed and receive advice on the participation in training courses or international missions.

The Defense Staff actively participates in various conferences or events on national security, the structures involved being directly interested in establishing clear policies and procedures on this issue. Among the most recent, we can list the following:

In March 2020, for a three-day period, Romanian troops belonging to the Special Operations Forces participated with their American and Polish counterparts in a training organised for the further development of the Aeronautic Personnel, an air-land integration training.

Another important event was the *"Black Sea and Balkans Security Forum"*, a regional security forum that brought in Romania special, experienced, guests in order to debate on the classical and emerging security challenges from Black Sea and the Balkans regions. During the event, there were panels on different topics, relevant for Romania and neighbouring areas' security.

In August 2020, at Hohenfels Training Center from Germany, the *"Saber Junction 20"* Multinational Exercise (SJ20) was conducted. 140 troops from the Romanian Armed Forces participated in this training. Exercise SJ20 contributes to the increase of European security and promotes stability in the region, by means of multinational training activities conducted by the allied and partner soldiers.

CONCLUSIONS

Human resources management is involved in the process of ensuring national security through several specialised structures with responsibilities in several fields, starting from recruitment, employment, integration, establishing a career plan, training and retirement.

Considering the new context of the security environment, it is important that, among the main objectives pursued by the Romania Armed Forces, to be the optimisation of the human resources management system.

Currently we are facing a complex and volatile security environment, which requires for the armed forces to be able to respond promptly and effectively and this is only possible through a performant career management.

BIBLIOGRAPHY:

1. Armstrong, M. (1991). *Personnel Management Practice*. London: Kogan Page.
2. Klatt, L.A., Murdick, R.G., Schuster, F.E. (1985). *Human Resource Management*. Columbus Toronto London Sydney: Merrill Publishing.
3. Mathis, R.L., Nica, P.C., Rusu, C. (1997). *Managementul resurselor umane*. Bucureşti: Editura Economică.
4. Torrington, D., Hall, T. (1995). *Personnel Management: HRM in Action*. London: Prentice-Hall International.
5. Presidential Administration (2020). *Strategia Naţională de Apărare a ţării pentru perioada 2020 – 2024. Împreună, pentru o Românie sigură şi prosperă într-o lume marcată de noi provocări*. Bucureşti: Monitorul Oficial, Part I, no. 574.
6. Human Resource Management General Directorate (2018). *Managementul resurselor umane în Armata României*, IInd edition, no. 14. Bucureşti: Centrul Tehnic-Editorial al Armatei.

WEBOGRAPHY:

1. http://www.cdep.ro/pdfs/buget/2020/nexa3/Ministerul%20Apararii%20Nationale.pdf, retrieved on 23.09.2020.
2. https://dmru.mapn.ro/pages/view/115, retrieved on 23.09.2020.
3. https://www.defense.ro/, retrieved on 26.09.2020.
4. https://english.mapn.ro/cpresa/5183_joint-training-exercises-of-the-romanian,-us-and-polish-special-operations-forces, retrieved on 26.09.2020.
5. https://english.mapn.ro/cpresa/5261_%E2%80%9Csaber-junction-20%E2%80%9D-exercise, retrieved on 26.09.2020.

COHERENCE, SYNERGY AND SUSTAINABILITY IN THE DEVELOPMENT OF THE ROMANIAN NAVAL FORCES IN THE MEDIUM AND LONG TERM

Captain (N) Ovidiu PORTASE

Romanian Naval Forces Staff

Changes in the environment where the Romanian Naval Forces operate determine the need for continuous adaptation and transformation to meet these conditions. The drafting of an institutional development strategy is a necessary, opportune action that ensures the imperative framework for coherent, synergistic, and sustainable development.

In this article, the author presents some considerations related to the structure and content, but also the drawing up and implementation process for a medium- and long-term development strategy, along with its applicability and impact on the Romanian Naval Forces.

The drafting of a medium- and long-term development strategy would ensure the single vision and synergy needed in the inititation and efficient implementation of all FNR initiatives, programmes, and development projects, useful elements not only to the FNR constituent members, but also to its collaborators, partners, and allies, elements that could pave the way for the convergence of efforts beyond the area of defence for the entire naval domain.

Keywords: strategy; transformation; development; naval forces; planning;

Motto:

"If we have a Navy and it is not needed, we would only lose money; if we do not have a Navy and we need it, we could lose the country".

Lieutenant Commander Gheorghe Mocanu (1943)

INTRODUCTION

The dynamism and transformations of the global security environment, as well as the recent actions of some state and non-state actors in the extended Black Sea region have generated a series of manifestations and effects that determine the need for paradigm shifts in national security and defence systems. One of the measures taken to adapt to new security situations and conditions is to adopt new strategies and policies in the area of defence or to modify existing ones, including changing the way in which instruments of power[1] are set up and used to promote and defend strategic interests.

This article has been written with the intention of presenting a series of arguments in an attempt to demonstrate that the drafting of a *medium and long term development strategy* (SDFNR) by the Romanian Naval Forces (FNR) is necessary and timely and that such a strategy would provide the FNR with the necessary framework for a coherent, synergistic and sustainable development, subsequent to the ongoing process of transformation and modernisation of the Romanian Armed Forces. The article also includes some considerations related to the structure, content and process of drafting and implementation of the SDFNR, as well as on the applicability and impact of such a strategy on the FNR.

The information presented in this article is for all those interested in the development of the FNR (at all levels, including the strategic planning level[2]). This information can be a common starting point in all discussions related to setting requirements for future FNR command structures, forces and capabilities and can contribute to the development of a common working base for those communities of interest acting in the area of concepts, doctrines, operations, capabilities development, procurement, and support.

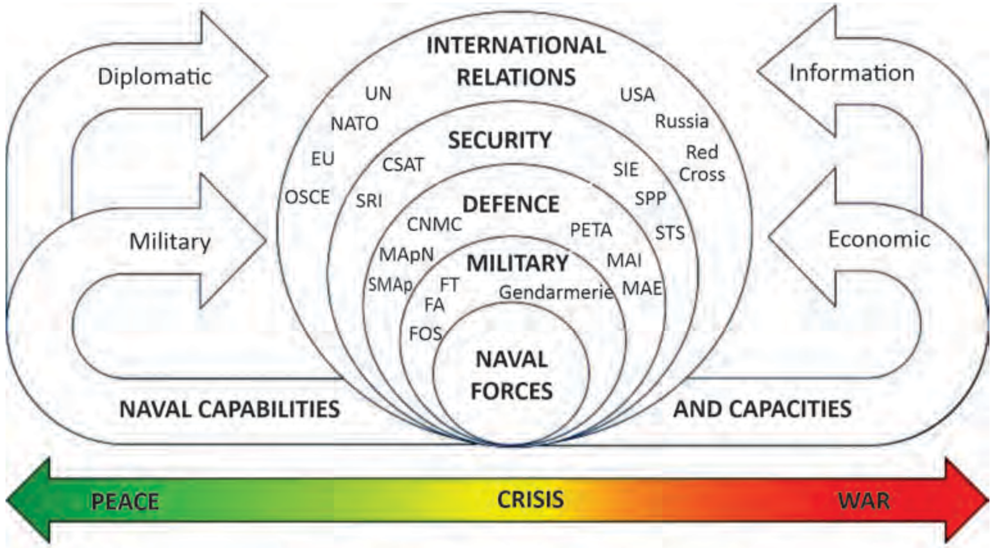
[1] Instruments of national power usually include diplomacy, information, military and economy (DIME).

[2] A coherent management framework for correlating public policies, budgeting, setting priorities, and managing an organisation's resources/organisational planning (http://www.mdrap.ro/planificare-strategica).

It should be noted that the term *strategy* is used in this article as the art and science needed for the institutional development of the FNR by setting out the desired final status, communicating it to the audience, determining the strategic approach, and identifying the authorities and resources needed to implement it (human, material, financial, temporal, etc.), as well as for the management of the risk associated with this development, without necessarily making a direct and exclusive reference to the process of planning and decision-making or of conducting military actions at the strategic level.

MIDDLE AND LONG-TERM DEVELOPMENT STRATEGY – NECESSITY AND OPPORTUNITY

The necessity for a medium- and long-term development strategy can be argued mainly by recent changes in the place, role, and missions of the FNR, by the need to adapt the structure of forces, capabilities, and their employment in the new conditions imposed by the strategic and operational environment, and, last but not least, by facilitating alignment of the FNR development directions with those existing at the national level or at the level of the North Atlantic Treaty Organization (NATO) and the European Union (EU).



CSAT – Supreme Council of National Defence
SRI – Romanian Intelligence Service
CNMC – National Military Command Centre
MApN – Ministry of National Defence
SMAp – Defence Staff
SIE – Foreign Intelligence Service
SPP – Protection and Guard Service
STS – Special Telecommunications Service
MAI – Ministry of Internal Affairs
MAE – Ministry of Foreign Affairs
FT – Land Forces
FA – Air Force

From the point of view of the main sector of activity, the place, role, and missions of the FNR are within the scope of national defence activities. One of the Romanian Armed Forces services, FNR contributes, along with other elements of the national defence system, to the implementation of the national defence capstone concept in the military domain and to the fulfilment of the Ministry of National Defence (MApN) attributions and responsibilities. In order to counter security threats that may come from the international maritime and riverine domains (terrorism, proliferation of weapons of mass destruction, piracy, illegal immigration at sea, etc.), especially after Romania's accession to NATO and EU, the FNR role has been extended beyond the traditional national defence scope. Subsequently, FNR has carried out new types of tasks and missions, such as those specific to maritime security (combating terrorism, asymmetric threats, anti-piracy etc.) and participated in multinational operations and missions such as Active Endeavour (2005), KFOR (2008), Black Sea Harmony (2009), Unified Protector (2011), Atalanta (2012), Sea Guardian (2016), Resolute Support (2018) and so on. At the same time, it should not be overlooked that, through activities conducted along with actors and entities belonging to the maritime and riverine related sectors of activities, other than defence (shipbuilding and repair, water transport, search and rescue at sea, maritime safety and security, naval diplomacy[3] etc.) and through the subsequent system of relations and interdependencies, FNR may be affected by or generate effects in sectors of activity outside the area of security and defence, therefore may be seen or act as an instrument and, why not, as an exponent of Romanian naval power.

The emergence of new dangers and threats, coming from state and non-state actors' actions (ISIL, Boko Haram, cross-border criminal organisations, etc.) and the shift in the actions and means they use demonstrate that the operational environment in which the FNR must act is very dynamic and continuously changing. Consequently, the FNR must adapt accordingly and develop its specific concepts[4], force structure, and employment in order to be able to make a contribution in counteracting these dangers and threats, as well as to fulfil their missions and tasks successfully.

[3] Public, cultural, and economic diplomacy achieved mainly through cooperation in the military and naval field to strengthen Romania's strategic profile, meet Romania's strategic objective in the field of defence, promote national interests, increase trust, and ensure regional security and stability etc.

[4] Institutional, operational, and functional, as they are set by the *Romanian Military Strategy 2016* (SMR 2016).

At the same time, the implementation of all strategies, policies and concepts applicable to the FNR without having a single vision nor its own strategy, to ensure alignment with the main evolutions and trends of each sector of activity manifested at a strategic level, could lead to a dissipation of efforts and inefficient spending of available resources. In this case, a SDFNR would ensure a holistic, synergistic approach – both vertically and horizontally, internally and externally – covering all areas; avoiding parallels, divergences or overlaps and combining efforts in the transformation and modernization process of the FNR. A SDFNR could also provide a common framework for discussion and work with other entities and organizations operating in the naval domain (Coast Guard, Romanian Naval Authority, Romanian Naval League etc.) which would provide the necessary conditions for a comprehensive approach at a national, or even regional, level, in which the FNR might have the leading role. At the same time, to deny the need for a strategy in the naval domain denotes the ignorance or rejection of the base principles stated by world renowned naval strategists, such as Alfred Mahan and Julian Corbett.

The opportunity to develop a SDFNR is given by a series of events and decisions, which are arguments proving that now is the right time for the FNR to develop such a strategy.

Thus, at the national level, the election of the new president of Romania in 2019 led to the initiation of the process of strategic analysis and drafting of a new set of defence planning documents (National Defence Strategy – SNAP 2020 and its implementation plan, Defence White Paper 2020, strategic defence analysis, military strategy, defence planning directive, etc.). In addition, in 2025 the last stage of the transformation process initiated by the implementation of the Romanian Armed Forces Transformation Strategy (STAR 2007) comes to an end the planning horizon of the current transformation, development, and procurement program will be reached (Romanian Armed Forces 2026). In all these cases, a SDFNR would provide not only the necessary foundation for formulating naval domain specific proposals and recommendations for future strategic planning documents (such as the reorganisation of the Romanian Armed Forces for multi-domain action until 2032 or the Armed Forces 2040), but also the continuity and stability element needed for medium and long-term implementation programmes and projects, and the development of new ones during the transition period from one political cycle to another.

The political decision to allocate 2% of Romania's gross domestic product for the procurement of the Armed Forces (*Acord politic național*, 2015) for a period of 10 years brings a significant increase in the amount of financial resources allocated to defence (implicitly FNR). Such a planning premise is itself an opportunity to initiate programmes and projects that require significant financial resources and/or need to run over a long period of time (such as infrastructure projects or mid life modernisation of large ships) or parallel modernization of several platforms and capabilities[5] (to reduce the time required to modernise the outdated platforms and equipment). At the same time, this major increase in funding for FNR programmes and projects combined with the widespread application of the offset procedure can be a serious incentive for naval producers and providers in Romania (shipbuilders, port operators, etc.), incentive that would have significant effects, some strategic, on the Romanian economy and population.

At the allied level, recent changes in the maritime operational context brought about by the development of new concepts and doctrinal documents (Allied Maritime Strategy – AMS, Allied Maritime Governance – AMG, Allied Joint Maritime Operations doctrine – AJP-3.1 etc.), the NATO command and force structure adaptation process (initiated in 2018) and the implementation of certain capability packages programmes and projects (IT Modernisation Programme, Broadcast And Ship Shore System – BRASS, TRITON maritime C2 services project etc.) must be seen as a major opportunity to establish new reference points and development directions for the FNR. In addition, the adoption of NATO's new architectural framework[6], which redefines the way future capabilities, systems, and equipment in NATO are modelled and developed, is a good opportunity to redefine the way requirements are set for future defence, military, and combat capabilities of Romania (and implicitly for the FNR).

The end of the 2016-2020 NATO Defence Planning Process (NDPP) cycle and the initiation of a new one, approximately at the same time as the national defence planning process cycle, should be seen as another opportunity, which will allow the orientations alignment and the convergence of FNR development directions for its forces and capabilities with those of NATO from the beginning. Similarly, the conclusion of the EU 2020 Strategy validity term and the possibility to have a new one released may be another favourable opportunity to draft and implement a SDFNR.

[5] According to the provisions of Law no. 203/2015, capability means the ability to carry out actions in order to achieve certain objectives. The establishment, development and maintenance of a capability envisages a complex of measures and actions in a broad perspective, including elements of doctrine, organisation, training, material, leadership, personnel, facilities, and interoperability (DOTMLPFI).

[6] The NATO C3 Committee validated NATO's new architectural framework (NAFv4) by the AC/322-D(2018)290002 document dated 25.02.2018.

The ones aforementioned are just some arguments in favour of the development and implementation of a SDFNR and to demonstrate that such strategy is necessary and timely. At the same time, to continue RNF development in the absence of such a strategy could lead to inefficient use of available resources, loss of opportunities, and partial fulfilment or failure in achieving the objectives of transformation and modernisation endeavour.

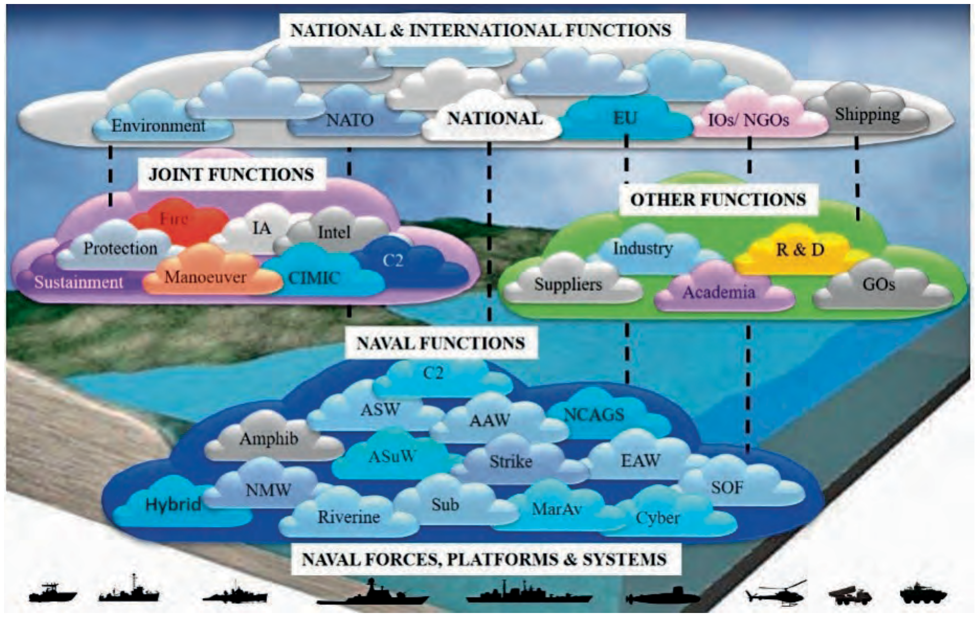
STRUCTURE AND CONTENT

The structure and content of the SDFNR depend mainly on the purpose for which the strategy is developed, the level of ambition[7], the FNR leadership vision on how the FNR will look and act in the future, and the approach used to turn this strategy into reality.

From a structural point of view, the SDFNR should include the context, vision, areas and directions of development, the resources needed to reach the desired final state and the implementation, monitoring, and evaluation mechanisms. SDFNR may also encompass those elements that describe the circumstances and conditions under which SDFNR is drafted and implemented, the current state of FNR, the finalities expected at the end of the strategy implementation period, the ways and means by which national military or non-military objectives will be achieved in the naval domain, as well as the criteria and priorities set out in the allocation of resources.

Given the current stage of the FNR transformation process and the tendency to move the centre of gravity on the development of new capabilities and capacities, it can be assumed that the main purpose of SDFNR is to provide the necessary framework, directions, and coherence for the FNR development process and its harmonisation with other similar processes.

SDFNR's purpose cannot be achieved in a realistic and efficient manner without a full understanding of the external and internal environment in which the FNR evolves and of the context for which this strategy is drafted and implemented. To do so, it is mandatory to take into account the characteristics of the security and operational environment specific to the naval domain (e.g. maritime threats, vulnerabilities and risks); key actors of this domain (stakeholders) and their interests; Romania's interests and objectives in the naval domain (including the level of ambition, requirements and priorities associated with them and so forth); the responsibilities, duties and authorities given to the FNR in the promotion and defence of naval interests; the place, roles and missions[8] of the FNR in national, regional and allied context; the institutional profile given by the national and international normative framework (laws and other legal norms specific to the security, defence, and naval domain; existing sectoral strategies and policies at local, national[9] or international[10] level; treaties, agreements and commitments to which Romania is a party, etc.). It should be emphasized that the FNR cannot be seen as an isolated entity or system, but as an organization belonging to several naval communities[11] at the same time and constantly interacting with other actors from different national, European, Euro-Atlantic or international communities. The complex character of the relations and interactions the FNR has with these actors of the strategic and operational environment determines the need for a strategic



[7] The level of ambition for the Romanian Armed Forces is defined currently by the 2020 Defence White Paper.

[8] These roles are explicitly described or can be deduced from national or international norms (e.g. roles according to national law: defence, crisis management, public diplomacy, supporting public authorities to ensure the vital functions of society; roles according to AMS: deterrence and defence, crisis management, security through cooperation, maritime security).

[9] STAR 2007, SMR 2016, Integrated Border Management Strategy, Sustainable Development Strategy – Regional And Territorial, Cyber Security Strategy, etc.

[10] NATO's Allied Maritime Strategy, Allied Maritime Security Strategy, EU Integrated Maritime Policy, EU Strategy for the Danube region, EU Strategy for the Black Sea etc.

[11] Maritime Enterprise and Maritime Compact in NATO; Maritime Clustersin some EU communities (https://webgate.ec.europa.eu/maritimeforum/en/node/3648) or System of Systems in system engineering.

approach to take into account all these elements, elements located – most of the time – out of the tactical framework.

SDFNR's vision must describe the desired end state at the completion of the strategy implementation process and express, in a broadly understood sense, the level of ambition for the FNR capabilities and capabilities needed in the future strategic and operational context. This vision serves as a source for reviewing/developing specific FNR concepts, for establishing how forces will be generated, employed and supported, as well as how FNRs will interact and collaborate with other entities. SDFNR's vision is an element without which the strategic planning of the FNR development cannot be executed (being indispensable for defining objectives, areas and directions of action, necessary resources and SDFNR implementation). This vision emanates from the future place, roles, and missions of the FNR and the minimum requirements associated with them (taking into account all public policies and sectoral strategies concerning the FNR) and must be eligible for evaluation, even if its components are not expressed quantitatively.

SDFNR objectives define the desired end state and establish the conditions to be met for the materialisation of the vision. The development of the FNR must have as a fundamental objective a modern force structure that is capable, integrated, efficient, flexible, deployable, sustainable, and fully professionalized with a high degree of mobility, having the capacity to be engaged in a wide range of missions and to operate jointly, both at home and abroad. SDFNR objectives fall within the main area of responsibility of the Ministry of National Defence - national defence, the secondary areas of responsibility (in which the Ministry of National Defence has a supporting role), and related areas of responsibility (which are influenced by or may influence the activities of the FNR); they are defined mainly based on the FNR's duties and responsibilities.

In order to provide the level of detail needed to understand the fundamental objective and to establish responsibilities in fulfilling it, it is desirable that the SDFNR points out general and specific objectives. These objectives may be specific to a particular area or direction of action or may be common to many. Among these objectives could be:

- completion of the transformation process started and based on STAR 2007;
- creating the necessary conditions for a coherent and sustainable development of the FNR (sound legal infrastructure; well-defined framework; increased institutional capacity, etc.);
- creation of a capable, flexible and adaptive naval force structure that meets the needs and requirements specific to the maritime, riverine, and related domains, that allows the fulfilment of tactical tasks and operational objectives;
- development of employment concepts and capabilities to guarantee the success of naval missions and operations whether they are executed independently, in cooperation with other state institutions or in a multinational context;
- strengthening and increasing infrastructure resilience in the maritime, fluvial, coastal, Danube Delta and lagoon areas, as well critical infrastructure located in the FNR area of responsibility or interest.

Generally, in order to ensure success in achieving these objectives, it is necessary to create certain conditions, which in the case of SDFNR would include:

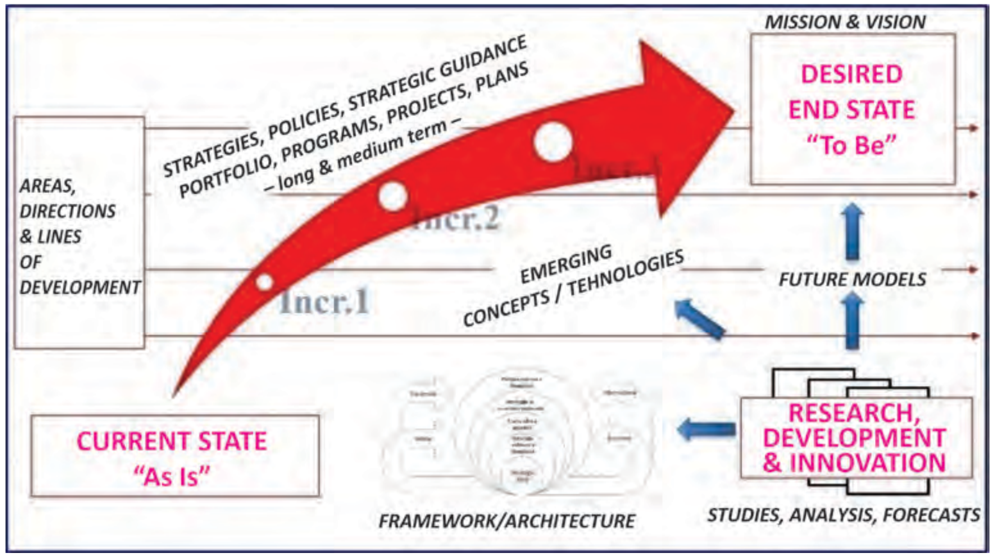
- raising awareness on the strategic importance of the development in the maritime and riverine domains and strengthening maritime conscience among strategic decision-makers;
- creating the normative, organizational and action framework necessary for the operationalisation of SDFNR;
- ensuring the long-term human, material, financial and other resources necessary for the execution of naval development activities and actions according to the level of ambition decided at strategic level;
- capitalising on all opportunities (political, economic, social, technological, etc.) applicable to the naval domain to promote the interests, values, and objectives of the FNR;
- the promotion and successful development of public-private cooperation at national level, as well as international cooperation in the area of maritime and riverine security.

After defining and describing the desired end state/ends through vision, objectives and conditions to be fulfilled, the next step is to establish the strategic approach, ways, means, and resources by which they are to be fulfilled.

The characteristics of the security and defence environment and their evolutionary trend, the joint and multinational character of the FNR missions and operations, and the complexity of the relations among entities operating in the naval domain recommend the adoption of a comprehensive, holistic, and incremental strategic approach based on a common framework.

The strategic nature of this approach is given by the SDFNR timeframe and by the need to take into account the contribution and influence on SDFNR objectives fulfilment of both the development of national defence system elements (command, defence forces, defence resources, and territorial infrastructure), and the evolutions occurred in all sectors of activity of the naval domain(maritime and riverine shipping, industry and shipbuilding, offshore energy facilities etc.).

The necessity for a comprehensive approach[12] is argued by the ubiquitous, continuous nature of FNR interactions with entities from within the area of defence and out of it and by the need for consultation, collaboration and coordination with them. FNR interacts with a plethora of national, allied and partner forces and/ or with various domestic or multinational entities of the maritime, fluvial or related domains, coming from both public and private sector regardless of whether it is capability development, service delivery, cooperation or other types of activities or whether it is during peacetime, crisis or war. The number and intensity of the interactions with these entities generate a series of peculiarities that must be taken into account when establishing the framework and directions of development.


MISSION & VISION
DESIRED END STATE "To Be"
STRATEGIES, POLICIES, STRATEGIC GUIDANCE
PORTFOLIO, PROGRAMS, PROJECTS, PLANS
– long & medium term –
AREAS, DIRECTIONS & LINES OF DEVELOPMENT
Incr.2
Incr.1
EMERGING CONCEPTS / TEHNOLOGIES
FUTURE MODELS
CURRENT STATE "As Is"
RESEARCH, DEVELOPMENT & INNOVATION
FRAMEWORK/ARCHITECTURE
STUDIES, ANALYSIS, FORECASTS

The complexity of the operational processes that take place at various levels of execution and the diversity of FNR relationships and interactions with the multitude of actors of the strategic and operational environment are real challenges in developing appropriate, viable conceptual models for FNR development. In turn, the specific features of the operational domains (air, maritime, land, space, cyber) and functional areas (human resources, information, logistics, communications and informatics, etc.) add another layer of complexity and bring a full set of challenges to those responsible for identifying and choosing optimal solutions to solve specific problems for each development direction. In order to eliminate the danger of divergent development trends and to allow the development of FNR in a holistic manner, it is recommended to adopt and implement a common framework (such as DODAF, MODAF, NAFv4, TOGAF[13], etc.) at FNR or a higher level, in order to use a single reference system, denominator for all the efforts made for FNR development. Thus, the analysis, design, planning, and implementation of SDFNR can be performed in the same way by all entities involved in FNR development, the level of integration, and interoperability of initiatives, programs, and projects and their subsequent products can be increased incrementally in each area, so development direction and resources can be used in a more efficient manner.

[12] The comprehensive approach is also mentioned by the NATO Strategic Concept and the AMS. At the same time, this approach allows the implementation of the concept of extended approach to national security, mentioned by SNAP 2020 and SMR 2016.

The areas and directions of FNR development establish the main areas of action, the principles, the ways, and the means by which the necessary conditions are created in order to fulfil the objectives, reach the desired final state, and achieve SDFNR vision. Given that FNR activities are mainly in the area of defence, it is desirable that areas and directions of FNR development are to be grouped around the national defence system elements (command, forces, resources and territorial infrastructure), thus ensuring SDFNR not only a sound legal basis – given by the defence fundamental legislative framework[14] – but also a great stability over time – given the minor changes brought to it throughout the last 15-25 years.

Generally, the development directions are initiatives characteristic of each development area, reflect the norms (laws, strategies, policies, etc.), concepts, and trends specific to each development area, being established mainly in relation to the FNR priorities. The measures and actions specific to each area and direction of action (programs, projects, plans, activities, DOTMLPFI solutions, etc.) will not be included in the SDFNR, in order to preserve the general character of the document. All of these should be detailed in the SDFNR implementation plan (PDFNR). Development directions may be specific to a certain development area (such as increasing the quality of human resources) or may be common to several areas (e.g. increasing

[13] DODAF, MODAF, NAF are architectural frameworks used by the United States Department of Defense, the United Kingdom Ministry of Defence and NATO, respectively. TOGAF is the framework agreed by the EU and Romania according to Government Decision (HG) 908/2017 for the approval of the National Interoperability Framework.

[14] Law no. 45/1994 on national defence, Law no. 346/2006 on the organisation and functioning of the Ministry of National Defence, Law no. 446/2006 on preparing the population for defence, Law no. 447/2003 on preparing the national economy and territory for defence.

the role of modelling – simulation in research, development & innovation – RD&I and in developing new concepts, strategies, doctrines and capabilities).

Some examples of SDFNR development directions could be:

a) in the command area:

- increasing command efficiency by clearly delimiting the administrative and operational chains of command and control (C2), shortening the duration of decision-making cycles, and delegating authority;
- ensuring the resilience of the C2 system by creating a network of modular, flexible C2 structures with a high degree of mobility;

b) in the forces and capabilities area:

- ensuring an optimal ratio of combat, combat support, and combat service support structures;
- maintaining a high level of readiness for force generating structures and deployable forces in order to quickly ensure the naval capabilities and capacities required for both the fulfilment of permanent missions and tasks, as for the planning, preparation, and when necessary, execution of extensive naval operations;
- organisational transformation of the FNR by implementing new naval concepts and including new types of naval forces and platforms (maritime aviation units, maritime unmanned systems – MUS, etc.);

c) in the resource area:

- allocation and use of resources based on initiatives, projects, and programs;
- adoption of multinational approaches and innovative solutions such as Smart Defence, Connected Forces Initiative, Pooling & Sharing, Framework Nation Concept, Permanent Structured Cooperation (PESCO) projects etc.;
- increasing quality in the process of the recruitment, selection, training, and use of human resources;
- building material stock and reserves and implementing a management system based on modern business tools, techniques, and procedures;
- planning, allocating, and spending financial resources on the basis of a multi-annual document with short, medium, and long-term provisions;

d) in the infrastructure area:

- increasing the level of cooperation with institutions with responsibilities in the area of critical infrastructure;
- carrying out port infrastructure programmes/projects jointly with the Ministry of Internal Affairs (MIA) and the Ministry of Transport (MT);

- improving the system of organisation, procurement, and training of the population, territory, and national economy to cover the FNR needs in case of war.

Although the SDFNR objectives, areas, and directions of action are mainly specific to the defence area, they can be complemented with provisions resulting from other national or international strategies related to the area of security and defence (allied, European, UN, regional etc.), naval domain or other areas related to FNR responsibilities and activities[15].

Along with the above mentioned structural and content elements, the SDFNR must also establish, in general terms, the resources and infrastructure necessary to fulfil SDFNR objectives, as well as the priorities and allocation of resources system, without providing details on their volume and sources, associated financial value or other planning and implementation data.

Even if the SDFNR is a general, high-level document, through its content, the SDFNR must provide all those data and information necessary to fully understand the purposes and means used to achieve the desired final state. Therefore, the structure and content of the SDFNR may include other elements, such as: values, interests, and objectives shared with other entities operating in the naval domain; assessments of the operational environment; vulnerabilities, risks, dangers, threats, etc.

Although it may seem an ambitious point of view, through its content, SDFNR can help systematise and unify the legislation and norms applicable to FNR, draw up FNR specific normatives and, within certain limits, influence or produce effects on strategic planning documents content. Therefore, great care must be taken in drafting SDFNR provisions in order to avoid falling into the trap of confusion between formulation of public policies, formulation of normative acts proposals, and strategic planning[16].

SDFNR DRAFTING AND IMPLEMENTATION

From the very beginning, it must be understood that the process of SDFNR drafting is a form of strategic art manifestation at FNR level, where strategic variables are analysed and taken into account in conceptualising how naval capabilities and capacities will be used in the future and where the directions, guidelines, and other

[15] As is the case with the National Strategy for Critical Infrastructure Protection, approved by HG 718/2011.

[16] See also HG 1076/2014 for theapproval of theStrategy on betterregulation 2014-2020http://www.sgg.ro/docs/File/UPP/doc/proiecte_finale/Strategia%20privind%20mai%20buna%20reglementare%202014%20-%202020_3%20decembrie_varianta%20finala.pdf

documents required to reach the desired final state are formulated. It should also be understood that this strategy should not be seen as an isolated, stand-alone FNR, but as a supporting document, a component of several higher-level strategies detailing the development of the naval forces and strengthening Romania's naval power, as well as how FNR, combined with other strategic elements (national defence industry, critical infrastructure, etc.), can contribute to the achievement of national or collective strategic objectives set at NATO, EU or other regional initiatives and coalitions level.

Drafting SDFNR can be done in accordance with the methodology and rules established for MApN normative acts or for republican level normative acts. If it is desired to ensure a high degree of commonality with the content and structure of documents developed by other ministries or if the scope of competences necessary for the drawing up and implementation of SDFNR exceeds the level of MApN competences, the use of government level terms and methodologies is recommended[17].

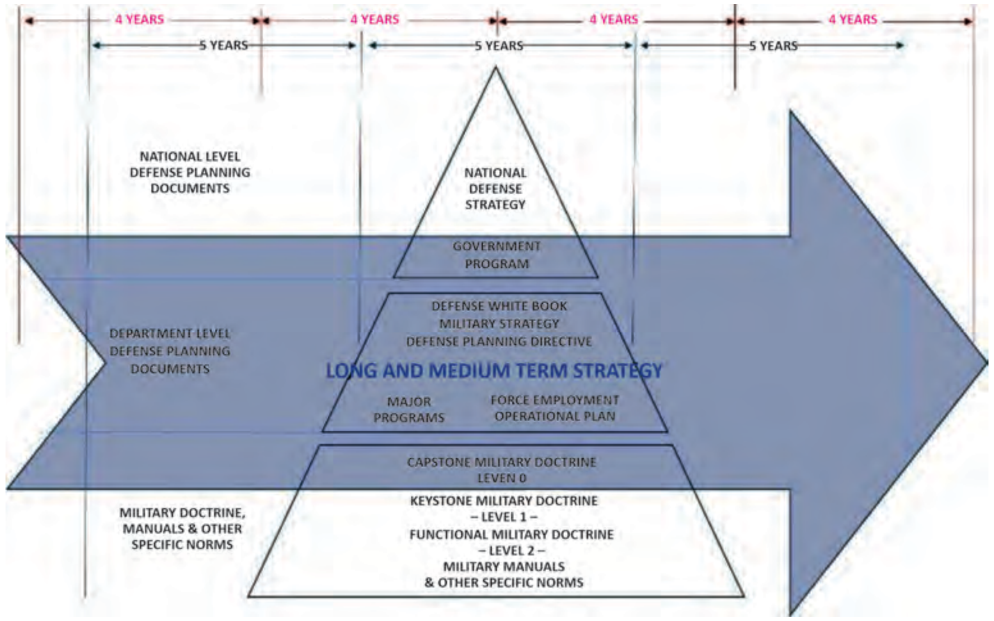
SDFNR drafting and reviewing process must be an ongoing process, based on continuous analysis of the strategic and operational environments, on how FNR operates now and in the future, and on those factors that contribute to or may influence the success of SDFNR implementation. SDFNR must be conceived and drafted taking into account the broader context described by various medium- and long-term strategies[18], in order to frame it within the general trend of the societal development and sectoral strategies[19] and to ensure the level of detail required for implementation. To ensure the modernity of SDFNR and to guarantee the viability of PDFNR, it is imperative to increase the role of CD&I throughout the entire process of drafting and implementing of SDFNR, especially in identifying and applying new concepts, models and technologies.

The first step in the SDFNR drafting process must be to study and analyse the strategic and operational environments related to the naval domain, in order to identify the characteristics of these environments and forecast the long-term and medium-term evolution trends. This studying, analysis and forecast (SAF) process

[17] According to HG 870/2006, the strategy is a medium- and long-term public policy document that defines, in principle, the government's policy regarding a certain area of public policies in which decisions on a widerange of issues are required. The strategy is developed in order to formulate a new public policy in the respective field, as well as in case thecurrent public policies need a significant improvement. Other applicable normative acts are HG 775/2005, HG 1807/2006, HG 158/2008 and HG 561/2009.

[18] Romania's development strategy for the next 20 years, Romania's national strategy for sustainable development 2030 etc.

[19] STAR 2007, SNAP 2020, SMR 2016 etc., and AMS, EU Strategy for the Danube region respectively.


4 YEARS
4 YEARS
4 YEARS
4 YEARS
5 YEARS
5 YEARS
5 YEARS
NATIONAL LEVEL DEFENSE PLANNING DOCUMENTS
NATIONAL DEFENSE STRATEGY
GOVERNMENT PROGRAM
DEPARTMENT LEVEL DEFENSE PLANNING DOCUMENTS
DEFENSE WHITE BOOK
MILITARY STRATEGY
DEFENSE PLANNING DIRECTIVE
LONG AND MEDIUM TERM STRATEGY
MAJOR PROGRAMS
FORCE EMPLOYMENT OPERATIONAL PLAN
MILITARY DOCTRINE, MANUALS & OTHER SPECIFIC NORMS
CAPSTONE MILITARY DOCTRINE LEVEN 0
KEYSTONE MILITARY DOCTRINE – LEVEL 1 –
FUNCTIONAL MILITARY DOCTRINE – LEVEL 2 –
MILITARY MANUALS & OTHER SPECIFIC NORMS

is carried out in order to establish the FNR place, role, and missions in the near and distant future – for different generic planning scenarios and the FNR full range of operations, in both a national and multinational context – and to define future FNR concepts, operating models, force structure, and capabilities applicable for the next 15-20 years.

In order to ensure continuity and coherence in the process of developing the FNR, the main national documents that must underlie the drawing up of the SDFNR are those that govern defence planning. The basic legal framework is established by Law no. 203/2015 – normative act that defines the main landmarks in the area of defence planning – and by the documents that substantiate the strategic planning at national and departmental level. However, it should be noted that these documents limit planning to a time horizon set mainly by electoral cycles (5 years for SNAP and 4 years for SMR, respectively) and therefore do not provide the necessary basis for medium and long-term planning. Moreover, although d efence planning directive resulted from the national defence planning process delivers the framework and offers the necessary guidance for major program directors[20] to adopt the best courses of action in achieving their specific objectives[21],

[20] The notion of major programme means, in the Ministry of National Defence, a programme as defined in Law no. 500/2002 on public finances – a coherent action or set of actions referring to the same main authorising officer, designed to achieve a defined objective or set of objectives and for which programme indicators are established to evaluate the results to be achieved, within the approved funding limits.

[21] https://www.mapn.ro/cpresa/15801_Directiva-de--planificare-a-ap%C4%83r%C4%83rii-2018-%E2%80%93-2027.

its planning timeframe (10 years) and scope are relatively limited and do not fully meet FNR programmatic requirements. Therefore, it can be appreciated that there is a need for an independent standalone document, which meets both the requirements arising from the defence planning process established by Law no. 203/2015 and other specific requirements, especially those related to medium- and long-term planning horizons.

Similarly, externally published documents, such as the NATO Allied Command for Transformation (ACT) report on the future strategic environment (SFA), respectively the framework for future Alliance operations (FFAO) report, the NATO Alliance maritime strategy (AMS), strategies published by countries and organizations with tradition in the naval domain (USA, Great Britain, France, Germany, Turkey, Russian Federation, EU), EU general scenarios on the future of defence[22], NATO generic defence planning scenarios based on mission types[23], the Romanian, EU[24], and UN goals of sustainable development, etc. should be taken into account in order to extend the level of complementarity and convergence.

The SDFNR drafting process must be strategically aligned with existing NATO and EU development directions and with the process, methodology, and content of the future NDPP cycle in order to enable the development of capabilities in a direction converging with those of NATO Member States and to ensure a higher level of technical and operational interoperability for an extended period of time.

A special role in drafting the SDFNR must be played by the structures whose CD&I or modeling-simulation (M&S) activities include or tangent the naval domain (specialized structures within FNR, MApN, NATO centres of excellence in the maritime domain, etc.). They can be co-opted in this process to prepare and make SAF products available, directly or indirectly, for the working group responsible for drafting SDFNR in order to ensure the scientific basis of SDFNR or they can help validate concepts of operations (CONOPS)[25], a preliminary, indispensable step required to initiate the development process for any new capability. Along with them can also contribute research institutes, centres and units, major economic agents operating in the naval domain, higher education institutes, employers, trade unions, professional associations, and other structures of civil society important for this domain (universities, autonomous administrations, research and development, etc.), under the conditions and terms set by law or other programmatic documents[26].

[22] According to EU document COM(2017) 315 dated 7 June 2017, *Reflection Paper on the Future of European Defence*, the three scenarios are: security and defence cooperation; shared security and defence; common security and defence https://ec.europa.eu/commission/publications/reflection-paper-future-european-defence_en

[23] NATO Encyclopedia, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_02/20190211_2018-nato-encyclopedia-eng.pdf, December 2018.

[24] According to EU document COM(2019) 22 dated 30 January 2019, *Reflection Paper Towards a Sustainable Europe by 2030*, https://ec.europa.eu/commission/sites/beta-political/files/rp_sustainable_europe_ro_v2_web.pdf.

[25] According to SMR 2016, the operating concepts define the application of military art and science and highlight the way the armed forces act in order to implement institutional concepts at strategic, operational and tactical levels.

Consequently, taking into account all the above, the SDFNR drafting process could include the following steps:

- analysis of the security, defence and operational environment at regional and global level, especially of the aspects related to the naval domain, using well-recognized methodologies (PESTLE/PMESII systemic analysis, internal SWOT analysis, operational analysis, etc.);
- drafting of the FNR vision for the year 2040[27] and of the main objectives to be fulfilled;
- establishing the framework and general concept of development, the stages and intermediate objectives, as well as the resources needed to achieve each stage;
- presentation and debate of the SDFNR project at the FNR doctrinal conference;
- revision of the SDFNR draft and its endorsement by the FNR Military Council and by the advisory forums of the upper echelons[28];
- approval of the final form of SDFNR;
- drafting of the SDFNR implementation plan, followed by its approval and execution;
- regular review of the SDFNR and its implementation plan.

SDFNR drafting process activities can be carried out by a FNR permanent working group (SDFNR Drafting and Implementation Working Group – GLEIS), made of specialists from all functional areas of the Naval Forces General Staff (SMFN), so all FNR command and force structures are represented. This group may consist, sporadically or permanently, of specialists from outside the FNR with whom it collaborates based on the agreements in force, thus forming an Extended Working Group (GLE), of inter-ministerial or interdepartmental type, to ensure the commonality and compatibility of SDFNR solutions with those specific to other

[26] Law no. 324/2003 for the approval of Government Ordinance (OG) no. 57/2002 on scientific research and technological development, HG 583/2015 for the approval of the National Plan for research-development and innovation for the period 2015-2020 etc.

[27] Planning horizon set by the 2020 Defence White Paper.

[28] Chiefs of Staff Committee, MApN College, Defence Planning Council etc.

entities and communities. If necessary, in order to develop the SDFNR and fulfil the necessary conditions for the drawing up of the overall concept, to ensure the coordination of its implementation in a holistic way at national level and to cooperate with non-governmental organizations that have attributions and/or carry out activities in the naval domain an Inter-ministerial/Interinstitutional Working Group (GLI)[29] could be established.

Given the general nature and the long time horizon of such a document, this strategy should be reviewed periodically, preferably every 5 years, whenever the change of documents underlying national defence planning (national/military defence strategy, white paper planning, the defence planning directive, etc.) or the emergence of new strategies and policies in the areas of responsibility of the FNR (AMS, AMG, etc.) occurs. The moment of strategy review is also an opportunity for the new FNR leaders to present their strategic vision, objectives, priorities, programs and projects.

The basic tool to ensure compliance with the operationalisation requirements set by the SDFNR and other specific strategies (STAR 2007, SMR 2016, etc.) is a FNR medium- and long-term development plan (PDFNR), a pro g rammatic document similar to an institutional strategic plan[30].

If SDFNR sets out the objectives, areas, directions, and lines of development, as well as the major stages of its implementation, then PDFNR will detail specific targets, measures and activities, their schedule, necessary resources, responsible structure, and its collaborators for each of them. In turn, it will serve as a basis for drafting the documents subsequent to those established by Law no. 203/2015 (the Naval Forces chapter in the procurement plans of the Romanian Armed Forces, Naval Forces major program, annual budgets, etc.), but also for all functional area plans issued to detail measures, actions and activities required by PDFNR implementation.

PDFNR will describe, broadly and in stages, the measures and actions to be taken in order to develop all necessary FNR capabilities and capacities planned for the period covered by SDFNR. Similar to SDFNR, the recommendation to use the language and methodologies specific to strategic planning[31] is preserved, as well as that to use the same set of fundamental concepts and documents (NATO Capability Hierarchy Framework – CHF, NATO C3 taxonomy, AMS, AMG, etc.) and their derivatives, thus enabling the alignment at concept and process level with the NATO maritime community and the achievement of strategic coherence in the maritime domain. Also, to ensure convergence in the implementation plan development process, it is recommended to use the same methodologies and analysis models (people-processes-technologies methodology, development line model and DOTMLPFI solutions) for all areas and directions of development. Only this way can be truly achieved the unity of effort necessary for synergic development on multiple domains and directions.

Obviously, such a plan must also refer to the non-military or dual – use naval capabilities and capacities necessary to fulfil FNR missions and objectives, but which are out of the Armed Forces responsibilities and for which the SMFN can be designated as the body responsible for providing expertise and assistance. One such case is the correlation of the provisions of MApN planning documents with those of departmental planning documents issued by different institutions, other than the MApN bodies (military units of the MIA or intelligence services, armed defence formations constituted by Law no. 45/1994, MT agencies, etc.) and which refer to naval capabilities and capabilities.

Unlike SDFNR, PDFNR must detail the allocation of resources and the system of priorities used for their allocation, as well as PDFNR implementation responsibilities. To this end, PDFNR should include multi-annual and staged resource planning guidelines needed for:

- identifying strategic and operational resource requirements and establishing the type and volume of material, human, and financial resources, as well as products and services needed for development during peacetime;
- establishing the level of reserves that will allow the continuous provision of resources, even under the conditions of a gradual increase of needs given by transition to a crisis situation or to a state of emergency, siege, mobilization or war;

[29] Similar to the Romanian Interministerial Group for the Integrated Management of the National Border established by HG 943/2001 (republished) based on HGR 750/2005 or the Interinstitutional Working Group for the protection of critical infrastructure established according to HG 1110/2010.

[30] The structure of such a plan, the working tools for its drawing up, as well as the way of organising the process of drafting, updating and approval of the plan may be similar to those described in the strategic planning manual published by the General Secretariat of the Romanian Government in 2009, http://sgg.ro/docs/File/UPP/doc/manual-planificare-strategica.pdf

[31] HG 158/2008, the materials drafted within the project *"Increasing the capacity of civil servants within MApN and ANFP to manage the strategic and project management processes, in the context of developing and strengthening the role of civil service"* and published at http://www.anfp.gov.ro/continut/Materiale_Proiect_SMIS_22857

- identifying the defence capacities[32] of interest for the FNR and establishing the measures and actions necessary for their continuous operation;
- adopting the necessary measures and actions to prepare the population, the national economy, and the territory for defence in accordance with FNR specific needs;
- drafting of programmes[33] and projects by which resources are generated, through the use of both domestic sources and imports;
- coordination at sectoral activities carried out to meet FNR demands and to prepare industry branches related to FNR for a state of mobilisation or of war.

Regarding SDFNR implementation responsibilities, it should be kept in mind that the appointment of those responsible should not be made only from those individuals acting in the area of strategic/operational planning or responsible for planning of structures and resources, as the development of the FNR does not only mean procurement. The development must be seen in a broader sense, therefore should also encompass the transformation and modernization from an organisational, information management, actional, etc. point of view by adopting/developing and implementing new concepts (e.g. maritime enterprise/compact, modern business and management models[34] etc.).

In order to guarantee SDFNR success, the SDFNR implementation plan must provide the necessary conditions to monitor and evaluate FNR development in relation to SDFNR. The process of monitoring and evaluating PDFNR execution and its revision differs from the SDFNR one, mainly through periodicity and level of detail at which they are performed. Monitoring and evaluating PDFNR execution involves the analysis of performance indicators established for its constituent elements. This could be done annually or at the end of a phase, in order to ensure that the evolution of FNR development stays within set limits, but also to avoid frequent changes and ensure the continuity and stability required for a coherent, sustainable development, the analysis and revision of PDFNR should be done as rarely as possible, preferably every four years[35]. Obviously, by exception, such an analysis can be made more often, when it is deemed necessary to set and implement measures and actions of an immediate nature (e.g. to adapt plan execution due to significant changes in annual budget allocations, or due to a sudden change of the fundamental planning documents generated by early elections).

[32] As defined by Law no. 447/2003 on the preparation of the national economy and territory for defence.

[33] A program is an action or a coherent set of actions that refers to the same main authorising officer, designed to achieve a defined objective or set of objectives and for which programme indicators are established to evaluate the results to be achieved, in the approved financing limits (Law no. 500/2002, MFP Order 1159/2004). FNR-specific medium-term budgetary policies and programs are financed mainly from the budgetary chapters for defence, education, health, culture, recreation and religion, insurance and social assistance, and general public services.

[34] Business administration, enterprise architecture, workflow, enterprise resource planning etc. applied in both administrative and operational activities.

[35] The same term (4 years) is the recommended duration for the strategic plans mentioned by HG 870/ 2006.

CONCLUSIONS AND PROPOSALS

The increasing importance of the Black Sea region in the current geopolitical and geostrategic landscape has generated an increase of the naval interests' weight in the equation of Romania's national interests and implicitly the need to develop those power tools required to promote and defend these interests. Successful fulfilment of the missions and objectives set for the FNR, in a strategic and operational environment with a continuous dynamic and characterised by an accelerated arms race, requires a permanent and sustainable development of the FNR.

In the absence of a programmatic document to set out, align and harmonize the FNR medium- and long-term development objectives and directions with similar documents of the naval domain issued at national, NATO and EU level, to ensure a common framework and the necessary continuity of the FNR transformation, modernisation, and procurement process during the period of 10 years of more than 2% of GDP allotted for defence expenditures, the drawing up of a SDFNR appears as a natural, necessary, and opportune action.

A document related to institutional development planning, SDFNR could ensure the coherence, synergy, and sustainability of all measures and actions undertaken to develop FNR concepts, forces, and capabilities under its specific planning conditions, including those imposed by the duration of naval platforms life cycles[36] or the financial value and the long term of naval infrastructure construction works, elements of planning that go far beyond the predominantly tactical level at which naval forces planning processes are viewed at and limited to or the planning horizons established by political election or NDPP cycles. Thus, such a strategy will not only provide the data and information necessary to substantiate FNR programs and subprogrammes, but will also ensure the necessary continuity in the drafting of proposals for subsequent medium-term programmatic documents – such as procurement plans, defence planning directive or future major FNR programs.

[36] The lifecycle of a naval platform exceeds 30 years and requires a major modernisation in the middle of the normal service life. To this duration has to be added the amount of time required to design, build and equip the platform.

In the form presented by this article, SDFNR is intended to be a programmatic document that supports strategic planning processes[37] - especially in the area of integrated defence planning for naval-specific issues that exceed SMFN competencies for public policies and budgeting (e.g. preparing the territory for coastal defence operation, ensuring the legal framework for ship requisition during a state of siege, emergency, mobilisation or war; imposing war piloting regime; waterway works, etc.) and provides the link among MApN public policies, tasks, priorities, and budgetary programs of interest to the naval domain and thus increasing efficiency in spending public money. The approval of a SDFNR at the national or sectoral level would increase the chances of carrying out major investment projects under the conditions provided by the Methodological norms regarding the prioritization of public investment projects (approved by HG 225/2014).

SDFNR could be a MApN internal document to support strategic military decision-making on FNR development matters and to provide the basis for interinstitutional cooperation in naval development (to some extent similar to the Cooperative Strategy – CS21 signed by US Navy, US Marine Corps and US Coast Guard leaders). At the same time, the SDFNR can become a document that facilitates the implementation of a sectoral strategy (such as STAR 2007 or SNAP 2020) or the correlation of existing provisions in specific documents from diverse sectors of the naval activity (shipbuilding and repairs, maritime shipping, defence etc.). Concurrently, considering its major impact on economic and financial realm, as well on the general consolidated budget, SDFNR can be a public policy[38] document that identifies solutions for solving public policy problems in the naval domain and source in the drawing up of domain specific legal acts.

The drawing up of a SDFNR would ensure the single vision and synergy needed in the initiation and efficient implementation of all FNR initiatives, programs, and development projects, useful elements not only to the FNR constituent members, but also to its collaborators, partners, and allies, elements that could pave the way for the convergence of efforts beyond the area of defence for the entire naval domain. Moreover, the drawing up of the SDFNR could be an opportunity for the FNR to become a catalyst and promoter of naval interests at national and regional level. Developed for a medium and long-term planning horizon and aligned with other national, NATO and EU strategies related to security, defence, military, maritime, riverine or naval domains, SDFNR can become the framework strategy of the FNR, a fundamental document that can be used as a basis for drafting FNR proposals for defence planning documents. At the same time, SDFNR can be a programmatic document that, made available to civil servants and policymakers in the naval domain by the MApN specialised body, can be used as an argument or support in developing, implementing, and evaluating public policies specific to this domain.

[37] Using the terms defined in Annex 2 of the Integrated Strategic Planning Methodology (HG 158/2008), SDFNR can be seen as a component of the institutional strategic plan of SMAp/MApN, PDFNR as a component of the strategic development plan, and the Romanian Armed Forces Procurement Plan (PIAR) as the operationalisation plan.

[38] According to art. 6 of the Regulation on the procedures for drafting, monitoring and evaluation of public policies at central level approved by HG775/2005 and the definition for public policies established by HG870/2006.

BIBLIOGRAPHY:

1. Locotenent-comandor Mocanu, Gh. (1943). *Strategia Mării Negre*. In *România Militară* Journal, no. 3-5.
2. Vlad, V.-I. (coord.) (2015). *Strategia de dezvoltare a României în următorii 20 de ani*. București: Editura Academiei Române.
3. *Acord politic naţional privind creșterea finanţării pentru Apărare*, https://www.presidency.ro/ro/presedinte/documente-programatice/acord-politic-national-privind-cresterea-finantarii-pentru-aparare-13-ianuarie-2015, retrieved on 12 September 2020.
4. AC/322-N (2016) 0021-AS1 – C3 Taxonomy (Baseline 2.0 – 2015). 11 February 2016.
5. AJP-3.1 – Allied Joint Maritime Operations. Edition A. (2016).
6. AJP-3 (C) – Allied Doctrine for the Conduct of Operations (2019).
7. AD 80-106 – Alliance Maritime Governance (2017).
8. Bi-SC 085-001 – Bi-SC Capability Package Directive 085-001, ed. 5 (2018).
9. C-M (2011)0023 – Alliance Maritime Strategy (2011).
10. Carta Albă a Apărării (2020).
11. Hotărârea Guvernului României nr. 158/2008 pentru aprobarea Componentei de programare bugetară din cadrul Metodologiei privind sistemul de planificare strategică pe termen mediu al instituțiilor administrației publice de la nivel central.
12. Hotărârea Guvernului României nr. 225/2014 pentru aprobarea Normelor metodologice privind prioritizarea proiectelor de investiții publice.
13. Hotărârea Guvernului României nr. 561/2009 pentru aprobarea Regulamentului privind procedurile, la nivelul Guvernului, pentru elaborarea, avizarea şi prezentarea proiectelor de documente de politici publice, a proiectelor de acte normative, precum și a altor documente, în vederea aprobării/adoptării.
14. Hotărârea Guvernului României nr. 583/2015 pentru aprobarea Planului naţional de cercetare-dezvoltare şi inovare pentru perioada 2015-2020.
15. Hotărârea Guvernului României nr. 718/2011 pentru aprobarea Strategiei naţionale privind protecţia infrastructurilor critice.
16. Hotărârea Guvernului României nr. 750/2005 privind constituirea consiliilor interministeriale permanente.

17. Hotărârea Guvernului României nr. 775/2005 pentru aprobarea Regulamentului privind formularea, monitorizarea și evaluarea politicilor publice.
18. Hotărârea Guvernului României nr. 870/2006 privind aprobarea Strategiei pentru îmbunătăţirea sistemului de elaborare, coordonare şi planificare a politicilor publice la nivelul administraţiei publice centrale.
19. Hotărârea Guvernului nr. 908/2017 pentru aprobarea Cadrului Național de Interoperabilitate.
20. Hotărârea Guvernului nr. 943/2001 privind înființarea Grupului Interministerial Român pentru Managementul Integrat al Frontierei de Stat (republicată).
21. Hotărârea Guvernului României nr. 1076/2014 pentru aprobarea Strategiei privind mai buna reglementare 2014-2020.
22. Hotărârea Guvernului României nr. 1110/2010 privind componenţa, atribuţiile şi modul de organizare ale Grupului de lucru interinstituţional pentru protecţia infrastructurilor critice.
23. Hotărârea Guvernului României nr. 1260/2011 privind sectoarele de activitate conform Legii nr. 62/2011.
24. Hotărârea Guvernului României nr. 1.807/2006 pentru aprobarea Componentei de management din cadrul Metodologiei privind sistemul de planificare strategică pe termen mediu al instituţiilor administraţiei publice de la nivel central.
25. Legea nr. 45 din 01.07.1994 – Legea apărării naţionale a României.
26. Legea nr. 203 din 16.07.2015 privind planificarea apărării.
27. Legea nr. 324 din 8 iulie 2003 pentru aprobarea Ordonanţei Guvernului nr. 57/2002 privind cercetarea ştiinţifică şi dezvoltarea tehnologică.
28. Legea nr. 346 din 21.07.2006 privind organizarea și funcționarea Ministerului Apărării Naționale (republicată).
29. Legea nr. 446 din 30.11.2006 privind pregătirea populației pentru apărare.
30. Legea nr. 447 din 12.11.2003 privind pregătirea economiei naţionale şi a teritoriului pentru apărare.
31. Legea nr. 500 din 13.08.2002 privind finanțele publice.
32. Legea nr. 51 din 29.07.1991 privind securitatea națională a României (republicată).
33. Manual de planificare strategic. Guvernul României – Secretariatul General al Guvernului (2009).
34. Ordinul Ministerului Finanțelor Publice nr. 1159 din 30 iulie 2004 pentru aprobarea Instrucțiunilor privind conținutul, forma de prezentare și structura programelor elaborate de ordonatorii principali de credite în scopul finanțării unor acțiuni sau ansamblu de acțiuni.
35. *Regulamentul privind procedurile, la nivelul Ministerului Apărării Naționale, pentru elaborarea, avizarea și prezentarea proiectelor de documente de politici publice, a proiectelor de acte normative, precum și a altor documente, în vederea adoptării/aprobării de către Guvern* din 05.03.2018.
36. *Strategia națională pentru dezvoltarea durabilă a României 2030*. (2018). București: Editura Paideia (adoptată prin HG 877/2018).

37. *Strategia de transformare a Armatei României* (2007).
38. *Strategia Națională de Apărare a Țării pentru perioada 2020-2024. Împreună, pentru o Românie sigură și prosperă într-o lume marcată de noi provocări* (2020).
39. *Strategia militară a României – Forțe armate moderne pentru o Românie puternică în Europa și în lume* (2016).

SHORT ANALYSIS OF THE BEGINNING AND USE OF BIOLOGICAL MEANS

Colonel Gabriela-Elena SÎRBU, PhD

"Carol I" National Defence University, Bucharest

Assoc. Prof. Vasile BOGDAN, PhD

"Danubius" University, Galați

Since immemorial time, armed confrontations made use of elements with biological potential for damage, which were already present in nature. The naturally occurring high-risk diseases were skilfully used to bring decisive operational advantages, thus tilting the victory to those who intelligently used the already existing possibilities in the environment. Gradually, with the development of technology and the impact of scientific research, biological factors of high impact on the living force were identified, developed and used in the operational space. The triggers of biological attacks are able to quickly cause serious illness and death of contaminated persons, as well as the decommissioning of targets and land. The action mode is generated by the ability to spread rapidly, achieved by dissemination in air, water or on the ground or by personal contact between individuals. Diseases that can be triggered by using them at critical moments or in carefully selected spaces allow reaching the specific objectives of the aggressor entity.

During a turbulent 20th century, deeply involved in a fierce competition for world domination, the great powers noticed the major destructive potential as well as the surprising operational innovations offered by the biological weapon. As a result, they switched to discreet and careful research, followed by testing of the advantages that can be obtained in armed conflicts, through the offensive use of the new weapon into the belligerent area. If, during the First World War, the significant concerns belonged to Germany and Great Britain, during the Second World War, the case of Japan must be given priority.

Keywords: biological agents; vulnerabilities; nuclear weapons; chemical weapons; decontamination; anthrax;

INTRODUCTION. ONSET OF THE BIOLOGICAL WARFARE

Infectious diseases have been playing a significant role in tipping the balance of victory during armed confrontations – a well-known aspect since ancient times. The potential for contamination was assessed so that it could be easily applied to the population or armies, depending on the circumstances. It is possible that the onset of making deliberate use of biological factors to have been marked by using bad-smell or deadly substances in their already existing natural state, as well as contaminated animal carcasses or long-dead fighters' corpses. By achieving unpleasant effects (illness or incapacitation), the end result was to weaken the belligerent ability of the opponent.

Thus, as widely used procedures, we mention the poisoning of wells and other water sources, so that the opposing army could not use them. The procedure of depriving the opponent of the necessary water support was widely practised by Romanian voivodes, among whom Ștefan cel Mare, Vlad Țepeș, Mihai Viteazul etc. That action possibility was a common tactic in campaigns carried out over time in Europe, Asia or America, even in the 20th century. In the Middle Ages, the contamination of water and food sources was widely used to harm the opponent with poisonous substances extracted from plants, a similar case being that of processing sword blades and the tips of arrows and spears.

In the Middle Ages, at the level of the army leaders, there was the practice of using the corpses of fighters contaminated with infectious diseases as offensive weapons, due to the included potential for contamination. In this regard, during the 1346 siege of Caffa (a solid fortified Genoese port-fortress, located in the current territory of the city of Feodosia, Crimea), the Tatar army did possibly use the biological weapon in repeated terms – which most likely was not a first at the time – a weapon represented by the plague[1], i.e. with producing an epidemic of bubonic plague. For all we know, it is estimated that the bubonic plague (or plague) had its first outbreaks in East Asia, possibly in China, India or Mongolia. The bubonic plague, known as the *Black Death*, devastated Europe and North Africa during the Middle Ages (14th century), being the most destructive pandemic recorded in world history. The Tatars knew the advantages of the created situation, turning some vulnerabilities of the Tatar army (insured by the deaths of their own fighters

[1] Plague is a very severe illness caused by the *Yersinia pestis* bacterium. Those contaminated have terrible pains, chills, fever and profuse sweating. At the joints of the limbs and neck, the victims develop swellings full of pus. At first, blisters are pink, then they turn orange and black at the end. Without a proper treatment, those contaminated can die in terrible suffering (A.N.).

because of the plague) into a decisive advantage, able to ensure victory. In order to incapacitate the defence device of the fortress, the Tatars catapulted in the besieged city the corpses of the Tatar fighters who had previously died of plague. Thus, in the crowded besieged fortress of Caffa, an epidemic of bubonic plague was quickly triggered.

The mass disease of the besieged fighters was followed by the Genoese defenders leaving the besieged fortress (Riedel, 2004, p. 400). Frightened and terrified by the mysterious situation of sickness that occurred, and without sensing the illness causes, the Genoese fighters hurriedly left the port city by sea. Nonetheless, all the personnel evacuated by sea had been contaminated by the plague. Following the disembarkation from the ships in different ports of Europe, the contaminated passengers transmitted the plague to the persons with whom they came in contact, achieving serial contamination throughout the whole Europe. Under those conditions, the biological attack on Caffa had extremely disastrous consequences in the future. The biological attack of the Tatars on the fortress of Caffa led to the spread of bubonic plague in Europe. Because of the plague, between 1/3 and 1/2 of Europe's population at that time disappeared as a consequence of the mass contamination of human communities (Ibid., pp. 400-401).

The case of smallpox as a biological weapon can be used as a procedure undertaken in the broad action of conquering the New World. Thus, for the contamination and decimation of the opponents, Pizarro offered to the native population clothes contaminated with the smallpox agent, the biological agents being masked in the form of offering gifts. In a similar manner and for similar purposes, in order to defeat the resilience of the North American Indians, the British offered gifts to the Indians, consisting of hospital blankets and medical utensils, the gifts being contaminated with the smallpox virus (Bogdan, 2016, p. 28). Synthetic information regarding the onset of using biological warfare in the past is presented in Table no. 1 (Riedel, Ibid.).

TABLE

comprising the main biological events produced at the beginnings of history (Ibid.)

Time	Event	Place
600 BC	Solon used hellebores inflorescences, having a purgative role.	The siege of Krissa
1155	Emperor Barbarossa ordered the contamination of water wells using human corpses.	Tortona, Italy
1346	The Tatar army catapulted over the walls corpses contaminated with bubonic plague in the besieged fortress.	Caffa, in Crimea
1495	The Spaniards used the blood of patients with leprosy to contaminate the wine that was offered to French opponents for purchase.	Naples, Italy
1675	German and French troops agreed to refrain from using poisoned projectiles (thus, previously used).	
1710	Russian forces catapulted corpses contaminated with bubonic plague into cities.	Sweden
1763	The British supplied blankets contaminated with smallpox to Native Americans.	The US territory
1797	Napoleon supported the creation of optimal conditions for the proliferation and spread of malaria, by flooding the lowland near the town of Mantua.	Italy
1863	Confederates sold clothes contaminated with yellow fever and smallpox agents to union troops.	The US territory
First World War	The Germans and the French used biological agents of glanders and anthrax.	France and Belgium
Second World War	The Japanese were using bubonic plague germs, anthrax bacteria etc. for operational purposes.	China, The Indochinese Peninsula
	Other states were developing biological weapon programmes.	
1995	The Aum sect used anthrax in Tokyo	Japan

Table no. 1: The use of biological means in the last two millennia

As it can be seen from the table above, during the Middle Ages, forms of biological warfare were generally isolated, the use of biological agents being without significant consequences in the balance of victory. As a paradox, the situation of the bubonic plague of 1346 in the fortress of Caffa (Crimea) should be highlighted. The Tatar army, which besieged the city without any chance of success, after using the corpses of contaminated dead human vectors, not only managed to conquer the fortification area of the defensive Genoese structure, but caused astronomical damage to the European continent that was devastated by the plague (involving the bacterium Yarsinia Pestis), as well as large territories in Asia and Africa (Greenspan, 2020).

ATTEMPTS AT OFFENSIVE BIOLOGICAL EFFORT IN THE FIRST WORLD WAR

The use of biological warfare agents increased in the concerns of armies with significant military potential during the 19th century. The growth was allowed by the achievements in the development of microbiology, the technological and scientific level facilitating the production of high quantities and diversity of pathogens.

Germany, the most heavily industrialised state participating in the world conflagration, was a promoter of using certain elements of biological warfare. The rather ambitious (relative to the possibilities of the times) biological programme refers to actions prepared by way of covert operations. Due to the easy-to-understand confidentiality, the details of the programme are not known exactly. Even in these conditions, we mention the German intention to send some livestock elements (especially cows and horses) infected with anthrax and glanders, the US being also placed among the targets. Biological agents were later inseminated to sheep, the animals being prepared for sale in an also covert manner within Russia. German attempts to spread cholera in Italy and bubonic plague in Russia (Saint Petersburg) may also be considered (Bogdan, Ibid., pp. 28-29).

As a conclusion, the states that won the First World War were placed in a dual situation. On the one hand, they progressively condemned the opponent's biological experiences. On the other hand, they secretly went on conducting biological research to determine and expand the destructive possibilities of the new type of weapon in the armed confrontations of the time.

A comprehensive diplomatic effort taken by the world's states was necessary – one aimed at stopping the proliferation of chemical and biological weapons, both of which are believed to be capable of inducing the mass destruction of the living force. The goal was achieved by the Geneva Protocol of 1925 (Riedel, Ibid.).

CONCERNS OF BIOLOGICAL WARFARE IN THE SECOND WORLD WAR

The states that did not comply with the provisions of the Geneva Protocol continued to develop ambitious research programmes and practices on biological warfare.

Japan made significant combat efforts, out of the desire to achieve world supremacy in Asia, the action being synchronised with the similar intentions of Germany, with a possible junction in the Middle East (the Persian Gulf). Starting in 1932 until the end of the Second World War, Japanese researchers were heavily involved in the issue of biological warfare. The well-known, famous, *"Unit 731"*, a large Japanese research/development and experimentation structure located in Manchuria, near the city of Pinfan, was used as a pivotal research structure. In conducting the research included in the Japanese Biological Warfare Programme, more than 3,000 researchers were active, with 150 buildings and 5 subordinate centres (Ibid., p. 401).

The main direction of interest in the research was aimed at using biological agents liable to induce in the belligerence area certain biological diseases (anthrax, meningitis, dysentery, cholera, plague) that were favourable to the Japanese attacker. In the analysis and evaluation of the particularities regarding the operational use, the complex tests required the use of heterogeneous and very numerous samples. Thus, the target group for testing was provided by approximately 10,000 prisoners of war. The prisoners were easy to ensure in the respective conditions, they favoured the conduct of discreet experiments, in order to easily achieve the considered objectives. Under the conditions of detention by the Japanese, the target group consisted of Korean, Chinese, American, British, Mongol, Russian and Australian prisoners as well as civilians. The research carried out was marked by excessive harshness and cruelty, without hesitation regarding the number of losses. In the biological experiments performed, more than 3,000 of the *"human lab rats"* available lost their lives (Bogdan, pp. 28-29).

New complex biological experiments on the use of the latest biological agents were undertaken in the Japanese biological research. The Japanese tested the possibilities of therodotoxin (poison with extremely high toxicity, produced by fungi), as well as the use of bubonic plague carried by fleas and rodents as transmitting agents. In the experiment regarding the use of bubonic plague, fleas were launched from the plane over Chinese cities, aiming to start plague epidemics. The experiments lacked biological protection measures in preconceived and total terms (i.e. notification, communication of wind direction, provision of protective equipment, manoeuvre to remove human entities from the movement direction of the biological cloud etc.) including for the Japanese troops. Under these conditions, for a biological attack on the Chinese city of Changten, at the total death toll of 10,000, there should have been added about 1,700 Japanese soldiers killed by fratricidal involvement.

In the period following the conclusion of the conflict, the accusations of the parties were reciprocal. Thus, a contingent of 12 Japanese prisoners of war was tried at a Soviet military tribunal in Khabarovsk in December 1949. The contingent consisted of former leaders responsible for the manufacture and use of biological weapons. Prominent among the defendants, Major General Kawashima, the former three-section commander of Unit 731, was charged with killing more than 600 prisoners. In response, the Japanese government accused the Soviet Union of experimenting with biological weapons (anthrax, cholera and dysentery). (Riedel, Ibid., pp. 401-402).

Germany knew particular but low-level concerns. Because of Hitler's traumatic experience during the First World War, in contact with chemical agents, Hitler stopped the development of the biological weapon[2]. In the absence of a direct support from the German dictator, the research effort did only benefit by little support coming from certain high-ranking Nazi figures. Under these conditions, the German offensive biological weapons programme could not materialise. In isolated situations, agents of hepatitis A and malaria appear to have been used to infect prisoners of war.

After the war, German officials accused the Allies of using biological weapons. Thus, Goebbels accused the British of attempting to spread yellow fever in India with the help of infested mosquitoes from West Africa. The accusation was credible and amounted to British concerns about anthrax testing in the vicinity of the Scottish coast. Because of the massive contamination of the experimental field, the decontamination of the environment was achieved only in 1986 with the help of formaldehyde and seawater. (Milton, 2005, pp. 61-63).

The *United States* launched the programme for research and production of offensive biological weapons in 1942 under the coordination of the War Reserve Service, which was in fact a civilian agency. The programme aimed at the use of anthrax[3] and Brucella suis[4] in the space of belligerence. The biological material was produced in Terra Haute, from the state of Indiana, and researches were conducted at Camp Detrick. The test sites were located in Mississippi and Utah. Approximately 5,000 bombs loaded with anthrax spores were produced to carry out the test effort. In order to continue the biological effort, the US Army Medical Research Institute of Infectious Diseases maintained its position and intense activity in Fort Detrick (Riedel, Ibid., pp. 401-402).

Certainly, the Second World War is at the height of research, extensive operational testing of *"human lab rats"* and the operational use of biological weapons.

The case of Japan is emblematic in illustrating the biological research that took place in a literally savage, inhuman way. The research work was particularly intense, a development of the field of research materialising realistic conclusions and consolidating a significant expertise. The moral authors of the research, testing and use of biological weapons were investigated, punished and subjected to public disgrace. It should also be noted that the results of Japanese research, the ways of working, the experience in the field, as well as the specialists migrated to the victorious states of the world confrontation. Those countries confidentially used the biological and operational biological elements taken from those defeated in order to invigorate their own future biological research, both defensive and offensive. Thus, the biological arms race continued, the main promoters being the two superpowers during the Cold War, the USA and the Soviet Union.

[2] Hitler considered chemical and biological weapons to have an absolutely inhuman potential, the reasoning having certain biographical connotations of the German dictator (A.N).

[3] Anthrax, also called *malignant pustule* or *woolsorters' disease* is an infectious illness induced by *Bacillus anthracis*, the disease being a zoonosis, therefore common to animals and humans (A.N.).

[4] The bacterium causes porcine brucellosis, a zoonosis characteristic of swine (A.N.).

AMERICAN BIOLOGICAL WARFARE EFFORTS DURING THE COLD WAR

In the years after the Second World War, the public received numerous articles on abominable cases generated by representatives of the armed forces who used biological agents.

The *US actions in Korea (1950-1953)*. During the Korean War, China and North Korea accused the United States of America of using biological agents against North Korea. As a result, in the following years, the USA officially announced its capabilities to produce offensive biological substances, but denied the use of biological weapons in Korean military operations. During the Korean War, the US programme was expanded with a new chemical weapons facility in Pine Bluff, Arkansas. The US credibility did suffer as a result of the non-ratification of the 1925 Geneva Protocol. Added to these allegations was also informing the public opinion about the offensive biological programme, including the suspicion of a disguised US collaboration with the former researchers of the Japanese Unit 731 (Bogdan, Ibid., pp. 30-31).

The *US Actions after the Korean War*. After 1953, a defensive (protective) programme was launched and completed – one focused on the development of countermeasures (vaccines, antisera, therapeutic agents), undertaken for the medical protection of troops against possible biological attacks. Later, in the 1960s, the research prioritised the creation of an offensive biological arsenal (consisting of pathogens, toxins, pathogens extracted from fungi). The purpose of the tests carried out included soft ways of action, taking into account the civilian dimension, with the submission for analysis of the possibilities of compromising crops and starving the population. At Fort Deterick, tests were conducted on the use of *Francisella tularensis and Coxiella burnetii*. For the relevance of the research conducted, agents were grown in massive enclosures, containing storage volumes of 1 million litres each. The purpose of the experiment was to determine the human vulnerability to pathogenic aerosols (Riedel, pp. 401-402).

In the next phase, researchers were involved in testing the effectiveness of vaccines, prophylaxis and therapy for possible biological means to be used.

In the offensive biological programme of 1942-1969, 456 cases of occupational infection were produced. However, the contamination rate was lower than the US national standards in the field, there being recorded an infection rate below 10 contaminations per 1 million hours of exposure achieved in the process of productive activity. Another 48 occupational infections occurred in different production or testing sites. It should be noted that all cases of infection were caused by the defensive tests performed. (Milton, Ibid., pp. 63-65).

Between 1951 and 1954, complex tests were conducted to assess the vulnerability of American cities. Thus, the target groups were the agglomerations of the massive cities (New York and San Francisco). Aerosols were discreetly dispersed over the two cities, there being evaluated the effects of the biological factor used, the dispersion methods, the effects of solar radiation and the impact of climatic conditions on the human body (Ibid.).

American biological concerns have given priority to the defensive side of research, without neglecting the offensive concerns. For understandable reasons, official evidence and statements of American offensive biological actions are missing. It should also be stated that the defensive desires are driven by the purely civilian side of the responsible authorities, as well as by the need to counteract the possible manifestations of adverse biological offenses, through reliable sanitary-epidemic measures. (Miller, 2005, pp. 11-17). In both cases, the defensive research was revealed to the public on a favourable path, being received as positive.

BIOLOGICAL WARFARE EFFORTS OF OTHER STATES DURING THE COLD WAR

Similarly and at the same time with the American experiments, states with high technical-military potential, such as Canada, Great Britain, France, the Soviet Union continued their own research in the biological field (Ibid.). The position of great power creates specific attitudes and a particular behaviour in international relations.

Great Britain. In 1951 it increased the organisational structure of the Department for Microbiological Research, having as reference the variant of 1947. Biological warfare projects were structured, insisting on the development of new biological agents with increased virulence, simultaneously with concerns for functionality, tactical use and target-use vectors. The testing, evaluation and optimisation of biological weapons took place in the Bahamas, the Lewis Islands, as well as in the waters near Scotland. In 1957 Britain decided to stop the offensive biological warfare research and destroy the stocks. It must also be said that British research continued on defensive biological coordinates.

The Soviet Union was simultaneously interested in testing both the offensive and the defensive biological aspects. The major efforts for the offensive field were made in the 1960s and 1970s. Notable in the technical literature are the Soviet accidental releases of biological agents, which occurred in the smallpox outbreak in Aralsk (1971) and in the outbreak of anthrax in Sverdlovsk (1979). (Dembek, Pavlin, Kortopeter, pp. 51-53). However, we note that the Soviet Union has always officially denied possession of offensive biological or chemical weapons (Bogdan, Ibid., pp. 215-219).

Official Statements after the Second World War:

- the press in Eastern European countries revealed data on the use of biological weapons by the United Kingdom in 1957 in Oman;
- China accused the USA of producing the cholera epidemic in 1961 in Hong Kong;
- The US and Colombian troops were accused by the USSR of using biological agents against citizens in Colombia and Bolivia in 1964;
- Egypt's use of biological weapons in the Middle East and the outbreak of the cholera epidemic in Iraq in 1966 (Riedel, pp. 402-403). Extensive US training in countering chemical weapons has been a constant since 11 September 2001.

The efforts of the global security organisation and the responsible political powers of the moment must continue to address issues of strategic interest, using the political tools, in line with priorities arising from the need for biological security and balance of tomorrow's world (Mackby, 2003, pp. 9-10). The special effectiveness of the biological weapon is well-known as compared to other mass destructive factors. We reconsider the fact that, depending on the case, the destruction of a given human crowd can be achieved by allocating \$ 2,000,000 – if it applies to nuclear weapons, \$ 2,000 – in the case of chemical weapons and only \$ 2 – if biological weapons are selected. Therefore, the cost/effects produced efficacy is sharply increasing in the imagined graph that would successively include biological weapons, chemical substances/mixtures and nuclear means (Păun, 2003).

During the Cold War, the main military powers developed a wide range of measures in multiple areas, aiming to surprise and defeat the opponent. The scale of research, the level of funding, the support of specialists and the results themselves depended on the policy adopted by the strategic decision-makers and top military planners.

CONCLUSIONS

During Antiquity and the Middle Ages, in the context of symmetrical confrontations (armed force versus armed force), the means of biological warfare were quite rarely used in isolated cases. There may have been several forms, ways and cases of use, the documents of the time being quite poor in that manner.

The First World War introduced innovative forms of belligerence of the time. In addition to the established use of firearms and explosives, other methods, such as chemical and biological weapons, were activated and used. The use for the first time elegantly evaded the provisions of international law, the customs of waging war, surprised the opponent and supported the achievement of strategic goals estimated by offensive international actors.

The Second World War saw a change in the list of the main protagonists of research and use of biological weapons. Japan was the most eloquent case in the biological field, presenting a high interest for the matter, allocating important resources specialists, technology, infrastructure, funds and other possibilities. Thus, the unlimited and unrestricted use by the specialists of Unit 731 of the human factor, consisting of prisoners of war, the homeless civilian population and even their own troops, is illustrative.

Soviet and American research, successes and failures were cleverly masked by the veil of protection afforded by military or state secrecy. Only cases of failure or biological crisis got known to the large public and the research segment.

The lack of an effective international verification framework for compliance with the provisions of the Convention on Biological Weapons does not allow the exchange of information on the stocks of institutions involved in microbiological activities. In order to prevent the arrival of dangerous microorganisms in possession of anarchic, malignant structures, the strains must not be transferred or transported outside the secure biological facilities. Dangerous strains must be stored in safe spaces or destroyed, in conditions of biosafety and biosecurity.

There are not enough protective and legal measures in the matter of biological threat. The focus will be on increasing the capacity for monitoring and surveillance, detection, sorting, isolation, diagnosis and treatment. Likewise, vaccines and therapies will increase the ability to respond to the threats of induced infectious diseases. There must be triggered and supported the concerns of security organisations and progressive states for achieving a common, balanced platform of effort, with possible courses of action in several directions (Mackby, pp. 11-13).

The above-mentioned issues were the subject of extensive and fruitful discussions, which led to the negotiation and adoption of the *Convention on the Prohibition of the Processing, Production and Stockpiling of Biological Weapons and Toxins and Their Destruction*, a document signed in 1972.

The current COVID-19 pandemic will have to activate and sensitise public opinion, political and diplomatic mechanisms, to expand and update the provisions of the 1972 Convention on Biological Weapons. The biological crisis in 2019 will have to lead to the adoption of a viable document, with a content appropriate to the multiple changes in the biological, offensive and defensive, to establish effective control measures in biological research laboratories, microbial storage spaces, experimental grounds, to impose tougher measures for deviations from the rules, quantifiable and verifiable measures. The enormous loss of life and material damage, the enormous setback in the forward progress of today's society requires future measures of severe biological control and extensive international cooperation in large-scale biological crises.

BIBLIOGRAPHY:

1. Ackerman, G.A., Moran, K.S. (2006). *Bioterrorism and Threat Assessment*, no. 22. The Weapons of Mass Destruction Commission, Stockholm.
2. Bogdan, V. (2016). *Bioterorismul*. Editura CentruluiTehnic-Editorial al Armatei. București.
3. Dembek Z.F., Pavlin, J.A., Kortopeter, M.G. Chapter. *Epidemiology of Biowarfare and Bioterrorism*. Fort Detrick. Maryland.
4. Greenspan, J. (2020). *The Rise and Fall of Smallpox*, https://www.history.com/news/the-rise-and-fall-of-smallpox, retrieved on 11 October 2020.
5. Leitenberg, M. (2005). *Assessing the Biological Weapons and Bioterrorism Threat*. Strategic Studies Institute, US Army War College, Carlisle.
6. Mackby, J. (2003). *Strategic Study on Bioterrorism*. Centre for Strategic and International Studies. Paris.
7. Miller, R.I. (2005). *The Impact of Quarantine on Military Operations.* USAF Countraproliferation Center. Countraproliferation Paper no. 31. Alabama.
8. Păun, L. (2003). *Bioterorismul și armele biologice*. București: Editura Amaltea.
9. Riedel, S. (2004). *Biological Warfare and Bioterrorism: A Historical Review.* Baylor University Medical Centre Proceedings. Vol.17, no. 4.
10. https://www.history.com/news/the-rise-and-fall-of-smallpox, retrieved on 11 September 2020.

RANKING OF REPLACING MEDICAL EQUIPMENT – AN ELEMENT OF THE RATIONAL USE OF RESOURCES –

Colonel George UDROIU, BEng, PhD Student

"General Doctor Aviator Victor Atanasiu" National Institute of Aerospace Medicine, Bucharest

Brigadier General Prof. Ghiță BÂRSAN, BEng, PhD

"Nicolae Bălcescu" Land Forces Academy, Sibiu

Colonel (r.) Prof. Toma PLEŞANU, BEng, PhD

"Nicolae Bălcescu" Land Forces Academy, Sibiu

Maximising the value of medical equipment, in the context of financial constraints in the health system and the ongoing demands of clinical staff for new acquisitions, as an effect of the accelerated pace of technological development, requires the implementation of prudent management of the replacement process of existing medical technology, by aligning with the strategic objectives of the medical organisation and the epidemiological context of the moment. The development of replacement lists for healthcare equipment and the prioritisation of replacement should be done by employing a system of scores/marks given to medical equipment following the evaluation of clinical and non-clinical factors, both quantitative and qualitative, considering health care unit benefit, social impact and the costs associated with operational support. This estimated planning process, augmented on the basis of data from the medical equipment inventory programme and the expertise of clinical engineering structures of the hospitals, is a dynamic tool for substantiating needs and optimising capital expenditures.

Keywords: medical equipment; life cycle cost; inventory; replacement planning; ranking; cost/efficiency ratio;

INTRODUCTION

The planning and allocation of financial resources for capital expenditures in a medical organisation is based, in addition to the tool for evaluating new technologies entering the market, on the mechanisms and the processes for prioritising the medical equipment proposed for replacement, once reached the end of the operational life cycle. Because no standard way of allocating these funds has been devised worldwide, between the purchase of new technology and the replacement of the equipment fleet in the inventory, there is only the recommendation that the annual budget allocated to investments in medical equipment to be 10% (Temple-Bird et al., 2005, pp. 119-120) of the replacement value of the medical equipment fleet, in terms of hierarchy to replacement, the recent decisions are based on the analysis of factors of reliability, safety, efficiency, logistical support throughout the life cycle and cost associated with their operation and maintenance, to the detriment of subjective choices of new medical staff acquisitions and unplanned and unjustified replacements of equipment with high operating and maintenance costs.

Sustainable strategies for replacing medical equipment are developed over a period of 8-10 years (average useful life of technologies in the healthcare system) and are mainly based on data collected by clinical engineering (CE) structures in health units throughout the life cycle of the equipment, by continuously monitoring the operation of the technology and its technical problems, the clinical results delivered and the financial efforts dedicated to operational support. The collection of this complex data is usually done with the help of computerised medical equipment management systems and is initiated along with the implementation of technologies in the health system, representing a mirror of the medical devices history and a powerful tool for planning and prioritising replacements.

PRIORITISATION OF REPLACEMENT EQUIPMENT – MEDICAL TECHNOLOGY PLANNING TOOL

In order to achieve the balance between the potential of existing technology, the rapid technological development of new equipment as well as the optimal operating costs and the overall efficiency of the healthcare system hospitals should constantly follow the medical market evolution, national and international regulation regarding banning some devices, the safety parameters of the operated equipment, the degree of operability and the reliability of the medical equipment, in the sense of timely identification of the moment of regression of the cost/efficiency ratio.

The replacement planning process requires a holistic approach from staff with responsibilities in medical equipment management, such as medical staff, clinical engineering structures, administrative and technical staff, information technology, finance and procurement (*figure no. 1*), being a systematic plan of evidence and data that can demonstrate the need for and support the final replacement and procurement decision.

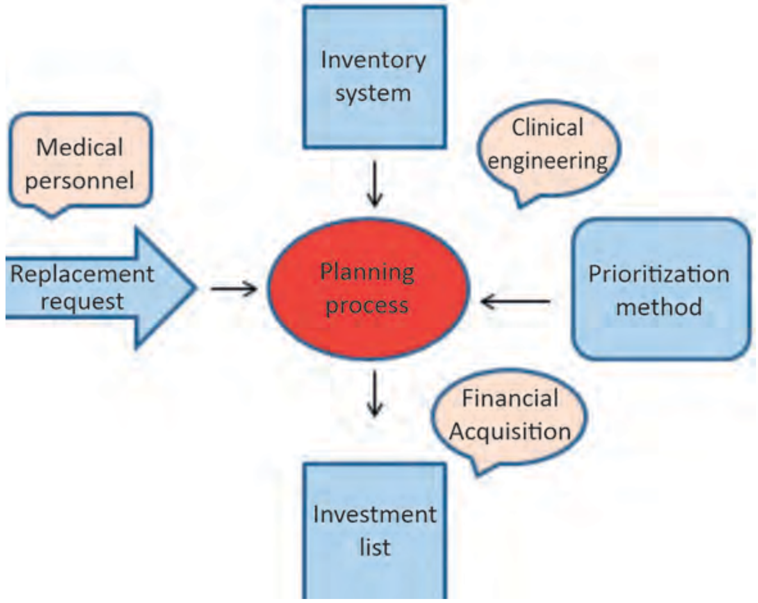


Figure no. 1: Structural components of the medical equipment replacement planning process

An ideal system for planning end-of-life medical equipment replacements should be developed based on the results of monitoring all vital and critical categories of equipment, and the analysis of clinical and economic profitability factors (medical benefits, safety, maintenance, costs, standardisation) should be done in the light of the three pillars of implementation of those more dynamic and flexible replacement plans, as follows:

- the package of strategic objectives of the health unit;
- the provision of quality medical services through safe and high-performance medical equipment, including market trends;
- the balance between estimating the life cycle costs of equipment and the rational allocation of support resources.

ASSOCIATION OF EVALUATED FACTORS FOR RANKING

In the practice of medical equipment management, several methods of prioritisation of technology replacement are known, based on the evaluation of *combinations of several clinical, cost, quantitative and qualitative factors* (Capuano, 2010, pp. 101-109) with impact on quality and costs. The division of the equipment is made by the scores obtained following the analysis of the factors and is based on both accurate information from the inventory programme of medical technologies and concrete data resulting from the technical expertise of clinical engineering structures.

The most common factors analysed internationally for prioritising the replacement of medical equipment are:

- The normal operation duration of the medical equipment and the amortisation period (Publication 946, 2008, p. 111) – average degree of prioritisation. We specify that the normal duration of operation of a computed tomography (CT) is 12-15 years (H.G. no. 2139/2004), but clinical engineering structures must plan and allocate additional costs for periodic updating of medical software applications, because CT technology can be outdated in a maximum of 8-10 years;
- End of equipment life (EOL – end of life) (*Medical equipment*, 2012, p. 14) or unavailability of maintenance services and impossibility of providing spare parts and consumables (EOS – end of support) – high degree of ranking. Manufacturers of medical technologies may withdraw their support for the equipment both in terms of technical assistance operations and in terms of the production of consumables and spare parts and accessories necessary for their operation. Usually, this data for withdrawal of support is provided to medical organisations at least 2-3 years in advance, in order to plan replacements or identify potential alternative sources of support (unsustainable for periods longer than 4-5 years). Another aspect that can lead to EOL is the withdrawal of the equipment from the medical market and the prohibition of its use, as a result of incidents in operation. It is also possible that the acquisition of new, more performing equipment with new software will no longer be interoperable with older equipment, although it has not reached EOL;
- Reliability – high degree of prioritisation. Quantify failures and corrective maintenance interventions over a period of time (usually using a reference period of one calendar year), considering that the inspection and preventive maintenance (IPM) operations are performed on time and completely in volume;

- Estimation of the physical life of medical technology – average priority degree. The physical life of a medical equipment is estimated by the clinical engineering structures in hospitals, based on their own experience or through professional interaction with other medical organisations, and is recorded in inventory programmes. This duration depends on the time of use of the technology, the skills of clinical users and the care shown for the equipment, the quality of consumables, accessories and spare parts used during operation and maintenance, the operating environment. On average, for properly operated and maintained medical equipment with original materials and parts, whose IPM work has been performed according to the schedules of the CE structures in the operational support plans, normal operating time may be extended without additional costs by 40%;
- The cost of maintenance works (ECRI Institute, 1997, pp. 4-12) – high degree of ranking. The assessment is made by reporting the total maintenance costs from a calendar year to the purchase price, by including materials, spare parts and labour/workload, these data being extracted from the cost reports of computer applications that manage the history of equipment inventory or inventory programmes. Both the costs of corrective maintenance operations performed on an outsourced basis and service contracts (monthly subscription type, including scheduled technical overhauls) and the total costs of technical assistance actions performed with hospital internal specialists will be taken into account;
- The total time of functional incapacity of the equipment – high degree of ranking. The periods during which the equipment is malfunctioning due to technical failures are taken into account, as they affect the hospital's ability to deliver healthcare services according to the basic mission and cause significant losses to the healthcare unit budget (especially for medical imaging technologies, radiology, laboratory analysers);
- The clinical efficiency of the equipment and the trust of the operator – average degree of ranking. The result of the calibrations and periodic tests performed by the clinical user may determine the quality of the results and the waiting times for their interpretation;
- The function of the equipment in providing health care services – average degree of ranking. The classification and scoring of the function of each equipment included in the inventory programme (high risk, life support, routine) (Fennigkoh, 1992, pp. 43-46) is done by determining the *critical score* (Kevin et al., 2005, pp. 37-41) of each medical device in relation to the other technologies in the programme. For example, it can be considered and established that a CT equipment is assigned a maximum score due to the absolute importance in ensuring the operability of the medical services of a hospital, while a pulse oximeter is assigned a minimum score. The other equipment in the programme will be ranked using scores located between the two extremes;

- Physical and moral wear of the analysed technology – average degree of ranking. Usually, this factor is analysed and scored by the competent CE structures based on their own expertise or following technical reports issued by specialised external service operators, which measure the technical condition of medical equipment and functional characteristics. In addition, it analyses the current technology on the medical market, the possibility of updating and modernising medical applications that provide equipment functions, and the compatibility of future potential new technologies with the medical network developed in the hospital (e.g. to ensure interoperability with medical equipment future cardiac ultrasound equipment must be compatible with certain standards – DICOM[1]);
- Degree of clinical acceptability (Faisal et al., pp. 55-63) – average degree of ranking. It is one of the most subjective factors evaluated in the process of planning the replacement of medical equipment at the end of life cycle, which is not based on the measurable technical and clinical performance of the medical device, but only on the preferences of clinical staff towards a brand or medical equipment manufacturer;
- Safety in the use of medical equipment – high degree of ranking. This analysis is based on data obtained from monitoring and examination/research of adverse events (Tobey, 2004, pp. 153-154), as well as potential hazards and risks associated with the operation of medical technologies (errors, alerts or any other equipment safety issues for which no solutions have been found). constitutes a maximum score for replacement);
- Standardisation of medical technology – high degree of ranking. Reducing the number of models and brands of medical equipment in a medical organisation is the most effective way to reduce life-cycle costs through the economic benefits of lower purchase prices and reduced costs of operational support (consumables and spare parts as well as maintenance operations,

[1] DICOM® (Digital Imaging and Communications in Medicine) is the international standard for the transmission, storage, retrieval, printing, processing and display of medical imaging information, https://www.dicomstandard.org/, retrieved on 10.09.2020

training and continuous training of end-users and technical structures, already familiar with existing models). In the case of the introduction of new technologies of the same type, from the same manufacturer, consumables and accessories, as well as component modules are compatible, and clinical applications and medical software will ensure interoperability with the computer system and electronic health records implemented at each medical structure;

- Degree of use/operation of the equipment – average to high degree of ranking. It analyses the times/number of hours of use of the equipment proposed for replacement or new investment (for example, if a refractometer is used 20 hours a year, by the specifics of the medical unit, and an electrocardiograph is used 4-6 hours daily, it is prioritised when replacing equipment with a higher degree of use. The existence of similar equipment or reserves of consumables and accessories necessary for operation will also be taken into account.

International regulations, clinical or technical standards – high degree of ranking. International bodies may prohibit the use of certain medical equipment which, although proven to be reliable and effective, poses a danger to contact or interaction with the human body due to materials in the composition of the equipment or the nature of the diagnostic and treatment procedures.

Thus, the key factors that must be subject to the evaluation and analysis of the Medical Equipment Management Groups (MEMG), in order to prioritise the replacement and issue the final decision, as presented in *figure no. 2*, are based both on accurate data from the computerised record system and on information and evidence from the experience of medical and technical staff and provisions of international bodies in the field of health care services.

In a first stage of the ranking, the computerised record system can issue preliminary reports with the priority equipment to be replaced, based on concrete data recorded during their lifetime, and then the qualitative factors will be analysed by specialised medical and technical staff.

The final stage of the ranking is represented by the evaluation of the implementation costs of the new projects and the financial benefits brought to the hospital, but also of the clinical advantages of the new technologies, in relation to the medical organisation strategy and market regulation requirements.

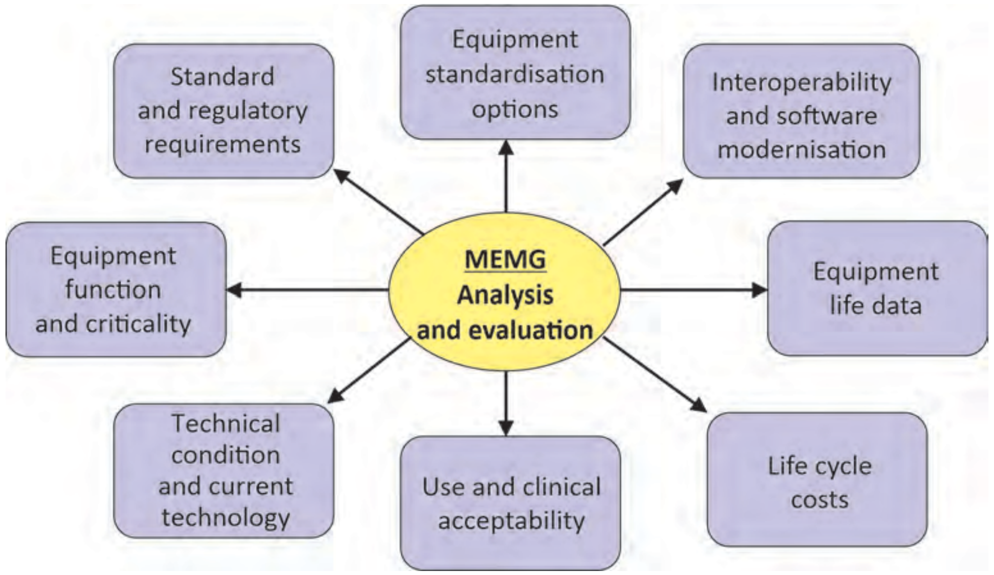

Standard and regulatory requirements
Equipment standardisation options
Interoperability and software modernisation
Equipment function and criticality
MEMG Analysis and evaluation
Equipment life data
Technical condition and current technology
Use and clinical acceptability
Life cycle costs

Figure no. 2: The nature of the factors analysed in the process of replacing medical equipment

As an example of classification and scoring in an evaluation, we present in table no. 1, the score that can be given following the analysis by risk categories (function, risk and degree of criticality).

Table no. 1: Example of risk categories evaluated in the prioritisation process (Ibid., p. 231)

Criteria	***Scoring***
Clinical function	
No patient contact	1
Device may make contact with patient but function is noncritical	2
Device is used for patient diagnosis, or direct monitoring	3
Device is used to deliver direct treatment to the patient	4
Device is used for a life support	5
Physical risk	
Device poses no appreciable risk due to failure	1
Device failure will result in low risk	2
Device failure will result in inappropriate therapy, misdiagnosis or loss of monitoring	3
Device failure could result in severe injury to, or death of, patient or user	4
Mission criticality	
Device is not important for patient care as care can be done via alternative methods	1
Device is important for individual patient care	2

Criteria	*Scoring*
Device is very important for one department	3
Device is very important for multiple hospital departments	4
Device is essential for overall hospital function	5

Throughout this replacement planning chain, part of the decision-making process to equip medical facilities, the contribution of CE structures through the permanent monitoring of the quality, safety, performance and costs associated with the use of medical equipment and the accurate recording of data is very important as well as reviewing them at appropriate times.

PROPOSED RANKING METHODS FOR REPLACEMENT IN THE LAST 30 YEARS

Accuracy of data recorded in computerised medical equipment management systems, robustness of programmes, time period and diversity of equipment included in monitoring procedures, access to official sources of information on the life expectancy of medical technologies and safety regulations for the use of equipment, as well as the knowledge and expertise of medical and technical staff are the most valuable resources that contribute to the development of plans for the ranking and replacement of medical equipment, based on quantifiable data and practical and scientific evidence.

If certain assessment factors have an absolute priority for replacement, such as operational safety, withdrawal of logistical support from suppliers or manufacturers (lack of consumables, spare parts, technical assistance) or exclusion from use by accredited bodies, the scoring of other factors can be done by means of calculation formulas, together with accurate data from the life cycle of medical equipment by setting maximum ranking thresholds, for example: the cost of a repair should not exceed 50% of the value of the replacement of the equipment, the total cost of the annual maintenance operations of the last 3 years should not exceed 25% of the purchase price, the physical life of the equipment should not exceed more than 30% of the normal operating time regulated by national provisions.

In the last 30 years, the methods by which medical equipment was proposed for replacement only by using written or computerised spreadsheets, based on inventory data obtained from the records of the hospital's medical departments, have evolved from procedures based only on age and life expectancy, plus the cost of replacement (Dondelinger, 2003, pp. 433-436), up to computer applications based on mathematical algorithms that can generate the year of equipment replacement, thus constituting a first form of short priority lists for replacement.

Since 1992, CE structures in medical organisations have developed equipment replacement plans based on the *Fennigkoh* prioritisation model, which focuses on the analysis of ten evaluation factors, using simple scoring formulas and covering the four major problems in the life of medical equipment: function, costs, maintenance and operational support (Fennigkoh, ibid.).

Subsequently, Malcolm Ridgway (2002) proposed a new method of prioritising the replacement of medical equipment, based on accurate data from the history of the equipment, its reliability and operating costs, using for evaluation a system of 7 factors in the life cycle of medical technology, as follows: age and operating status, degree of use, reliability, cost of annual maintenance, availability of consumables and spare parts, timeliness of existing technology and clinical acceptability. In the case of this ranking method, the total replacement score of each medical equipment is composed of the sum of the individual scores awarded to each evaluation factor (on a scale from 1 to 10 points), and the final ranking of prioritisation is in descending order of final scores.

In the same year, Binseng Wang (2002) promoted a new prioritisation method, based more on the economic return on alternative investments, recommending that, after analysing the equipment's operational status, operational support capacity and compliance with clinical standards, estimates should be made of the financial impact and return of new capital expenditures, as many medical technologies are proposed by medical staff for replacement, although they operate at nominal technical performance and in standard safety parameters. This method of prioritisation uses the life cycle cost model and the concept of current net value, as a percentage of expenditure, relative to the profit margin of the medical organisation.

In 2004, Robert M. Dondelinger proposed a new replacement method, complementing and strengthening the prioritisation procedure promoted a year earlier, based only on the life expectancy of medical equipment and the cost of replacement. The new approach becomes more complex and includes in the analysis and evaluation matrix new elements (Dondelinger, 2004, pp. 26-31), such as: age of medical equipment, number of corrective maintenance interventions/orders (repairs), total cost of maintenance operations, current (advance) of medical technology, such as and the adequacy of the technology to the objectives of the medical organisation for the next 5 years, thus giving a final score to each medical equipment, according to the scoring formula based on reports and percentages.

In 2010, Mike Capuano introduced a prioritisation system developed on the basis of a hierarchical index, the result of a combined assessment of factors, such as: price factor, current condition of medical equipment, availability of support to the provider/manufacturer throughout the life cycle, the age factor of the medical technology, the cost factor of the spare parts (as a percentage of the purchase value of the equipment), the risk factor (the risk level is updated in databases of the medical organisation), as well as the frequency of use of the equipment. Following the evaluation, these factors are scored with scores from 1 to a maximum of 6 points, each factor being subsequently applied a weighting index in order to distribute the importance of each factor, obtaining a ranking order based on distinct criteria, scores and weights.

On the model of such a method, in a health unit from the Ministry of National Defence internal network, a scheme for evaluating medical equipment was designed, in order to prioritise their replacement and draw up the short list, part of the final list of annual investments. The scheme includes a series of 7 factors to be evaluated, both objective and quantifiable, based on the data entered in the Register of medical equipment in use (Order no. 308/17 March 2015), mandatory by all health units in Romania, and subjective, based on the preferences of medical and technical staff. According to the algorithm, each factor is assigned a score, between 1 and 5 points, as shown in table no. 1. The final ranking coefficient is represented by the arithmetic mean of the weights of the evaluated factors, weights that can be established by recording the individual opinions of MEMG or another management group constituted at the level of the health unit, including medical and administrative staff, technical, financial and procurement, as detailed in table no. 2.

Table no. 2: The weight of factors assessed in the prioritisation process

Evaluated factor	**Points awarded**	**Weight**				
	1	**2**	**3**	**4**	**5**	
Condition (C)	Very good	Good	Acceptable	Weak	Very weak	0.13
Age (A)	≥5 years	≥8 years	≥10 years	≥12 years	≥15 years	0.155
Lifecycle Operating Support (LOS)	Fully insured	Partially insured (≥ 5 years)	Acceptable (2-5 years)	Inacceptable (≤ 2 years)	EOL	0.189
Annual maintenance cost (MC)	<5%	5%<CM<10%	10%≤CM<15%	15%≤CM<20%	≥20%	0.175
Degree of use (U)	≤2 hours a day or less	2<U≤4 hours a day	4<U≤6 hours a day	6<U≤8 hours a day	>8 hours a day	0.123
Clinical acceptability (A)	Totally accepted	Suitable	Accepted with upgrades	Requires auxiliary components	Unwanted	0.125
Function (F)	Others	Analytical support	Diagnostic	Therapeutic	Vital equipment	0.103

In the last 10 years, with the accelerated increase in the number of medical devices in use (3.7 million in 2018/Bernard, 2018) and simultaneously with the promotion of connectivity of medical equipment to various networks, in order to transmit and exchange clinical information and warning or failure data as well as *ensuring clinical interoperability*, methods of prioritising the replacement of medical technologies bring to the top of the priority lists medical equipment that requires major upgrades or upgrades to clinical applications, computer networks or even healthcare infrastructure, the costs of which would not be justified economically speaking.

Two other issues that have been addressed as a priority in recent years for the preparation of replacement plans are the analysis of patient safety factors, in the context in which, in 2018 in the United States of America, there were more than 5.000 deaths (Tobey, 2018) caused by improper design of medical equipment, technical failures of equipment and misuse by medical staff, and the vulnerability of medical equipment in terms of its cyber security and medical networks implemented at local, departmental or national level, given that more than half of health facilities worldwide believe that such a cyberattack is always possible on the equipment used in the hospital (Medical Device Security, 2017).

Today, while medical organisations in developed countries around the world use various computerised management programmes to manage the life cycle of medical equipment, preliminary replacement lists are generated automatically, and equipment prioritisation decisions are made easier and much better informed. The configuration of these monitoring and control systems allows CE structures to periodically obtain replacement year determination reports, based on accurate data and practical evidence, results of analyses of combinations of factors, such as: age, risk factors, normal duration life expectancy, average life expectancy, withdrawal from use (absolute factor – prohibition by international or national regulations), acquisition costs (come in support of the decision to replace with another new technology), operating and support costs (consumables, spare parts, accessories, maintenance work), EOL and EOS, decommissioning costs (estimates, similar equipment). These reports, revised by the CE structures by taking into account additional factors (standardisation, market trends, possible software upgrades and additional costs, cybersecurity issues, interoperability), are submitted to MEMG and subsequently to the Hospital Boards, in order to issue final replacement decisions, part of the management plans, in accordance with the basic mission and strategic objectives of the medical organisation.

CONCLUSIONS

Ranking of end-of-life medical equipment replacement is a powerful tool for life-cycle medical technology planning, based on the contribution of robust computerised management programmes that include a wide range of equipment and data over time their use, as well as the knowledge and experience of medical and technical staff, in terms of the functions, condition, trend, policies and costs associated with the use and maintenance of equipment in the healthcare sector.

The combination of factors selected for evaluation and the weights given to each factor are non-standard decisions of each medical organisation, but the priority system for replacement must be based on accurate and quantifiable data structures from the life of medical equipment, extracted from accurate inventories implemented by clinical engineering structures of the healthcare units, on clinical and technical evidence, such as safety, reliability or cost-effectiveness, but also on reliable information from other official sources of information (collaborating hospitals, departmental structures, national or international bodies, standards or guidelines).

Objective replacement plans, developed through a systemic approach to the whole process and algorithmic assessments of absolute and relative factors in the life of medical equipment, contribute significantly to optimising public health spending, reducing unplanned and unscheduled (accidental, emergency) procurement, improving the safety and quality parameters delivered by medical technologies, increasing clinical performance, as well as increasing the value of medical equipment in the context of current budgetary constraints in the global health sector.

BIBLIOGRAPHY:

1. Capuano, M. (2010). *Prioritizing equipment for replacement*. In *Biomedical Instrumentation Technology*, 44 (2).
2. Dondelinger, R. (2003). *A simple method of equipment replacement planning*. In *Biomedical Instrumentation Technology*, 37(6).
3. Dyro, J.-F. (2004). *Clinical Engineering Handbook*. Elsevier Academic Press. Burlington, USA.
4. Faisal, M., Sharawi, A. (2015). *Prioritize Medical Equipment Replacement Using Analytical Hierarchy Process*. In *Journal of Electrical and Electronics Engineering (IOSR-JEEE)*. Vol. 10, no. 3.
5. Fennigkoh, L. (1992). *A medical equipment replacement model*. Journal of Clinical Engineering, 17(1), Quest Publishing Co.
6. Iadanza, E. *Clinical Engineering Handbook*. Second Edition. Elsevier Academic Press, London.

7. Ridgway, M. (2002). *Preliminary Equipment Replacement Planning Report*. Presentation at the Advanced Clinical Engineering Workshop, San Jose.
8. Taylor, K., Jackson, S. (2005). *A medical equipment replacement score system*. Journal of Clinical Engineering, 30(1).
9. Temple-Bird et al. (2005). *How to plan and budget for your health care technology*. *How to manage series of health care technology guides*, no. 2. St. Albans. Ziken International (Health Partners International).
10. Tobey, J.C. (2018). *Adverse event notification, investigation and regulatory reporting in the United States, Global Forum on Medical Devices*. World Health Organisation.
11. Wang, B. (2002). *Repair, replacement and retirement criteria for health equipment*. Presentation at the Advanced Clinical Engineering Workshop. Guayaquil Ecuador.
12. ECRI Institute. (1997). *Medical Equipment Planning*, Health Devices.
13. Government Decision no. 2139 on 30 November 2004 to approve the Catalogue regarding the classification and normal life cycle of fixed assets, published in Monitorul Oficial no. 46 on 13 January 2005, București.
14. Synopsys, *Medical Device Security: An Industry under Attack and Unprepared to Defend*, Ponemon Institute LLC, 2017.
15. US Department of the Treasury Internal Revenue Service tax guidelines/ Publication 946, *How to Depreciate Property*. Modified Accelerated Cost Recovery System (MACRS) for 2008 returns.
16. https://www.dicomstandard.org, retrieved on 12 August 2020.
17. https://www.forbes.com, retrieved on 12 August 2020.

THE GENERATION AND ROLE OF THE 1972 CONVENTION ON THE PROHIBITION OF BIOLOGICAL WEAPONS

Colonel Gabriela-Elena SÎRBU, PhD
National Defence University "Carol I", Bucharest

Assoc. Prof. Vasile BOGDAN, PhD
"Danubius" University, Galați

In the first half of the twentieth century, the humankind experienced two devastating global conflagrations that caused millions of victims. The killer vectors were the destructive effects of firearms and, to a lesser extent, death was brought by terrifying actions utilising combat gases and biological agents. During the Cold War, the great military powers of the world continued their efforts to produce, develop, and store biological means meant to secure their victory in future wars. As a result, the spectrum of biological threats had to be reduced, and relaxation measures were taken. The Convention on the Prohibition of the Development, Production, and Stockpiling of Biological Weapons and Toxins and on their Destruction, a document signed in 1972, has the undeniable merit in this respect. However, it must be acknowledged that this Convention was not the first step taken. Previously, in 1925, the Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous and Other Gases, and of Bacteriological Methods of Warfare was signed. Although the effectiveness of this Protocol was low, the importance of such initial agreement is huge, as it opened the road to biological disarmament, and to increasing trust among nations. Arguably, following the severe Covid 19 pandemic, the 1972 Convention needs measures, policies, and actions to substantiate the desire of powerful states to gradually and totally eliminate biological arsenals worldwide.

Keywords: biological factors; disarmament; protocol; microorganisms; critical technologies;

> *Motto:*
> *"The single biggest threat to man's continued dominance of the planet is the virus."*
> Joshua Lederberg, PhD,
> Nobel Prize Laureate

INTRODUCTION

Scientific research on security environment describes biological impact, and, implicitly, biological weapons and bioterrorism as events or phenomena which may occur at any time, with unpredictable size, frequency, and consequences. History offers relevant, if not ample records of biological incidents. Certainly, biological events having afflicted the social and natural environment did occur in the past.

A biological crisis should be considered as a severe attack against human community security, due to vital resource contamination, critical facility damaging or physical destruction of numerous populations, following hostile or irrational actions. Biological challenge has the potential to activate a hard-to-measure destructive drive, with possibly catastrophic effects, and such disaster can occur in instances when the humankind fails to act intelligently, timely and in synergy. Through many supporting factors, the biologic agent dissemination is easy and quick. Globalisation supports rapid transmission of biological agents at large distances. Therefore, the pathogen biological impact factor presence is difficult to detect in due time, in view of implementing counteraction measures. The efforts of responsible authorities must be centred on surveillance and information, prophylaxis, detection, intervention, and treatment actions, isolation, and containment measures, as well as other measures pertaining to biological crisis management (Miller, 2005, pp. 10-11).

The history of war offers a plethora of cases where elements of biologic warfare were used by combatants to achieve their goals. The option of utilising the biological means stems from the threat vectors' destructive potential, which is massive, and difficult to prevent. Given that the biological agents were microorganisms, the contamination factors were easily used as biological weapons in battle. Biological agents allowed Middle Ages, or even earlier age armed forces to achieve specific objectives. Biological weapons host a destructive potential surpassing the destructive possibilities of conventional or even chemical weapons, by their directivity towards live force. Easy utilisation, wide utilisation range, low production and dissemination cost, plus the impossibility of effective counteraction by unprotected warriors or human communities make just a few of the issues which pushed towards international measures on banning the production, stockpiling, and utilization of such warfare means (Bogdan, 2016, pp. 27-28).

THE 1925 GENEVA PROTOCOL

As a nation participating in the First World War, Germany possibly conducted scientifically – operational activities in the field of biological warfare. It seems that Germany nurtured the desire to transfer infected livestock (with anthrax and glanders) to the United States and other enemy nations. Cattle and horses were transfer vectors, while infected sheep were used for livestock exports to Russia. There were also intentions by Germany to send cholera to Italy, and bubonic plague to Russia (to Sankt Petersburg). Germany also committed a biological bombing against British troops.

Germany adamantly rejected accusations regarding any activity of biological warfare and was successful in that endeavour. In 1924, after the end of World War I, a Nations League subcommittee was unsuccessful in the attempt to identify watertight evidence of the use of biological weapons in that global confrontation. However, the investigation commission was able to prove the utilisation of chemical weapons during the then recently ended WWI.

No doubt, there was an outstanding success for humanity. Various chemical and biological warfare implications, with specific consequences, resulted after WWI, and both warfare options were considered as potentially afflicting huge impact on human lives in an open conflict. Therefore, political and diplomatic efforts were necessary to stop further proliferation of such mass destruction weapons (Riedel, 2004, p. 401).

The *Geneva Protocol* appeared as a historical need stemming from the chemical and biological horrors of WWI, and negotiations unfolded under the League of the Nations aegis, in the framework of the League's main goal of preventing war. Consequently, on 17 June 1925, the *"Protocol banning the possession and use of asphyxiating, poisonous and other gases in warfare, as well as the ways in which bacteriological warfare should be waged"* was signed in Geneva, Switzerland. The document is also known as the *"1925 Geneva Protocol"*, and bears the signatures of 108 nations, including the five permanent members of the present UN Security Council. The United States began the ratification of this document only in 1975. Due to lack of agreement on clear measures regarding the implementation of a severe control, in the line of trust and verification, the worldwide applicability of Geneva Protocol was limited.

The gaps in Protocol applicability and control were speculated by several signatory countries, even after the document was ratified in those countries. For example, Belgium, Canada, France, the Netherlands, Poland, Japan, Soviet Union, and United Kingdom continued efforts in biological weapon development programmes (Bogdan, Ibid, p. 29).

THE NECESSITY OF AN AGREEMENT BANNING BIOLOGICAL WEAPONS

After the end of the Second World War, German officials circulated accusations against the Allies for having used biological weapons. It is known that, following Hitler's personal intervention (he had suffered from battle gas effects during WWI), the German offensive biological program was terminated (Riedel, Ibid, pp. 402-403). Practically, Goebbels accused the British of attempts to disseminate yellow fever in India, by using infested mosquitoes brought from Western Africa, as transmission vectors. The German accusation is credible, because it would follow previous British efforts, such as London's actions of testing anthrax on Scotland shores. Due to massive contamination of Scottish soil, complete environment decontamination was achieved as late as 1986, when formaldehyde and sea water were used.

The United States initiated its offensive biological weapon production program in 1942, under coordination of a civilian agency, the War Reserve Service. The American program focused on anthrax and *Brucella suis* (bacteria which causes swine brucellosis). The necessary biological material was produced in Terre Haute, Indiana, and research was conducted in Camp Dietrick, Maryland (Bogdan, p. 31). The Japanese Imperial Army infamous actions in Manchuria are well known: Unit 731 committed unimaginable atrocities in the war zone, against Chinese war prisoners and civilian population (Riedel, pp. 401-403).

In the big picture, the humankind acts extremely sensitive after the appalling slaughters committed during WWII. Following the post-WWII specific vibe, the general public and experts expressed criticism regarding the major epidemiological risk generated by the unpredictable and indiscriminate utilisation of biological warfare assets, as well as regarding the lack of any possibility of adequate epidemiological control over biological weapons. These concerns were based on the lack of valid, trusted, and directly verifiable information about national program statistics of several countries possessing biological warfare potential. The seventh and eighth decades of 20th Century recorded significant progress in international understanding and détente. The whole world strongly felt the need for a climate of calm and trust, for achieving wide area geopolitical balance, for progress in disarmament, as well as for diminishing the high-risk arsenals worldwide. There was a general desire for a more predictable world, committed to build peace and cooperation among nations, even among potential adversaries (Bogdan, pp. 31-32).

Countries possessing high-level technological and military capabilities were in obvious disagreement regarding the Geneva Protocol stipulations. The document was certainly proving its low level of practical effectiveness (Riedel, p. 403). Facing quite concerning biological realities, the UN Disarmament Committee noted the massive advance in offensive biological weapons, in opposition to lower progress in protective, defensive systems. Hence, it was clear that mankind showed high vulnerability to the massive biological potential of destruction accumulated by numerous international actors. In these circumstances, it appeared absolutely necessary to establish the measure of banning the development, production, and stocking biological weapons. It was also necessary to introduce control and on-site verification measures strongly needed in cases of breaching the internationally agreed prohibitive measures.

THE 1972 CONVENTION BANNING BIOLOGICAL WEAPONS

In September 1969, the United Kingdom initiated a series of framework proposals to Warsaw Treaty member nations, in view of diminishing the biological danger. After several consultations within the Warsaw Treaty, East-European countries sent to the United Nations constructive proposals leading to banning the biological weapons. Of course, that action was possible and unfolded under Soviet Union supervision.

The document was a continuation of older desires and disarming efforts of the entire progressive humankind and should generate the elimination of fighting methods totally rejected by the world. Therefore, the necessary starting point was supposed to develop stipulations written in the 17 June 1925 Geneva Protocol, that banned the use of toxic, breath taking and associate poisonous gases, as well as the use of bacteriologic means in military campaigns. Obviously, these measures had to be extended in the new document wording. Thus, by signing the future Convention, significant steps had to be decided for establishing a true and ample disarming worldwide, including by establishing practical control measures on the types of weapons used for mass destruction (Bogdan, pp. 33-34).

Against this background, in 1972, the *"Convention on the Prohibition of the Development, Production, and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction"* was adopted. The document strongly stipulated the banning of development, processing and stockpiling pathogen agents or toxins in quantities exceeding the needs for scientific research. According to this document, research was meant to be conducted only for prophylactic objectives, for protection, and for other purposes in direct support of peace. The draft convention included the banning of sale, technology, or expertise transfer to various countries, for other purposes. Thus, the convened document promoted the end of production, improvement, possession or stockpiling collection of pathogenic agents and toxins. Biological samples exceeding the minimal needs for research in this field had to be recorded and notified by quantity. Both the presence of stocks and biological weapon destruction process had to be controlled by effective measures, in transparency, under accepted international supervision. Additionally, immediately after the ratification of the treaty, signatory parties were committed to destroy stocks of biological materiel, distribution system and production equipment thereof, in a reasonable nine-month established timeline.

This historical agreement was possible by the consensus of 103 nations, and the *Convention* was ratified on 10 April 1972. It is worth mentioning that signatories who did not ratify the *Convention* offered their commitment to refrain from conducting activities in contrast with the goal of this agreement, until an official notification regarding the intention of not ratifying the document. Reviews of treaty stipulations were made in 1981, 1986, 1991, and 1996. As a deterrence measure, the *Convention* signatory parties had to communicate genuine data on facilities where activities pertaining to the document unfolded (biological research for defensive purposes, scientific conferences in venues under the incidence of the treaty, experience exchanges, focus groups, information transfers, other events with biological profile). Communications on such issues had to be made annually.

Ratification instruments and documents on new membership were to be deposited by the governments of United Kingdom of Great Britain and Northern Ireland, United States of America, and the Union of Soviet Socialist Republics, designated as depositary nations of the *Convention*. The agreed document was written in English, Chinese, French, Russian, and Spanish, as equally valid documents, the official papers being stored in Washington, London, and Moscow. Legally certified copies of the *Convention* were sent to the governments of signatory nations, as well to those governments who adhered to this agreement.

THE WORLD AFTER THE 1972 CONVENTION

It is interesting to see the evolution of the countries that developed biological programs or activities in biological weapons, as result of a specific dynamics. It is worth mentioning that numerous breaches of the international agreement unfolded in an increasing number of such countries:

- although they proceeded to ratify the Convention, in 1972 there were only four countries to have finished the ratification procedures;
- in 1989, ten countries were conducting biological activities;
- in 1997, twelve countries were in breach of Convention stipulations;

- in 2001, thirteen countries were conducting biological activities (Gould, Folb, 2002). Even in official documents, the United States position was somewhat ambiguous. Although the effort focused on the defensive issues of biological warfare activities, the offensive research was intended too, obviously for national security reasons. It is true, the divide between the offensive and the defensive domains, even for monitoring purposes, appears to be difficult to establish, because there is a common segment of initial scientific effort. Even the final divergent developments include plenty of elements which allow the migration of the real contents of a biological activity, obviously for propaganda reasons (figure 1) (Leitenberg, 2005, pp. 71-73). Clearly, during the next years, the number of countries having eluded 1972 Convention stipulations increased.

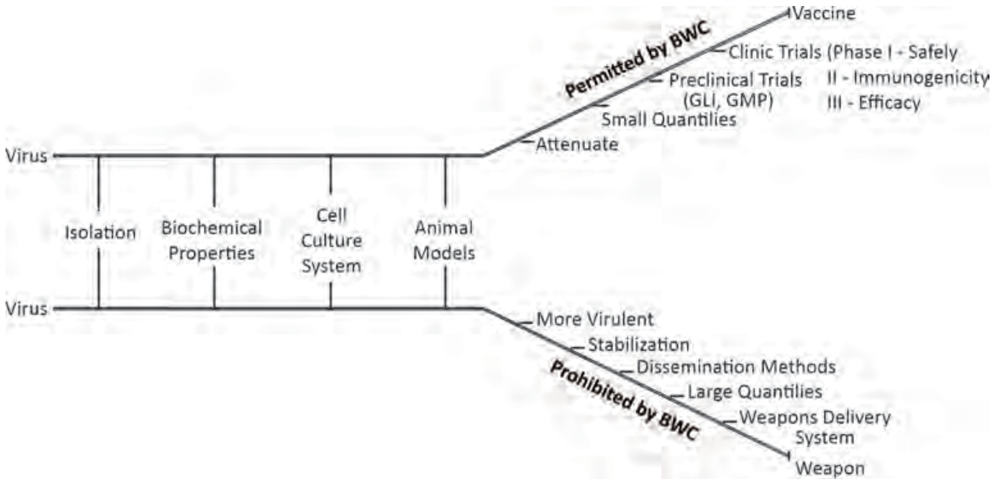


Figure 1: Common laboratory techniques (hypotheses) (Leitenberg, 2005)

The collapse of the Soviet Union and the Warsaw Pact termination (1991) increased general concerns regarding the protection, control, and responsibilities of entities possessing biological agents and other mass destruction weapons, plus associated materials, and technologies. The same, arguable concerns appeared, and they stemmed from potential unemployment and from the migration of thousands of scientists or specialised personnel towards areas of instability and future risk for the peace of mankind. It is known that biological attacks can cause catastrophic numbers of victims. After the collapse of the Soviet Union and the Warsaw Pact, in the conditions of the chaos within the Red Army, there was little control to establish the kinds of biological weapons that should not leak to the black market or unauthorised hands. The danger was certain and high, as the offensive biological substances could reach in the hands of extremists or terrorist organisations. Also, universities and research centres conducting medical research with various dangerous bacteria, toxins, and pathogen substances were potentially lacking sufficient security measures. Therefore, destructive biological factors are very vulnerable to stealing from hospitals, universities, research or testing facilities, and from stockpiling and decommissioning facilities. Anarchist organisations might intend to extend the size of their attacks by indiscriminately damaging more event scenes (special events, periodically or occasionally crowded spaces, high value targets, to contaminate wide areas or to widely spread the infection) (Bogdan, pp. 35-36).

The September 11 attacks in the US should be remembered also for the distribution of letters contaminated with anthrax spores during the week following the terrorist attacks, through the US Postal Service. Due to domestic incidents regarding the utilisation of anthrax since 2001 to the fall of 2003, American authorities used $ 7 – 8 billion in counter-bioterrorism programs. This money was necessary for damage control and for efforts meant to restore the level of biosecurity at national level. Earmarking such funds was meant for protection against the terrible bio-terrorist possibilities which may occur in the future. Further efforts and funds constantly increased thereafter (Leitenberg, pp. 65-67).

In December 2002, after the occupation of part of Afghanistan, the United States identified indications and data demonstrating that al-Qaeda was interested in purchasing knowledge and technologies pertaining to biological agent production (Mackby, 2003, pp. 6-7).

It is worth mentioning that, between 1989 and 1992, the Soviet Union breached the Convention regarding biological weapons, because, after ratifying the Convention, in 1975, it proceeded to develop a massive secret program on biological weapons, perhaps the largest in the world (Biological Weapons, 2000).

- The use of biological weapons or agents by terrorist organisations or non-state international actors seems to be very convenient, because:
- They can generate victims in mass numbers, the destructive agents can elude legal control, as the substances have dual use.
- Hostile entities intend to overwhelm the governmental system's emergency response capability, regarding the biological crisis.
- They brutally disrupt human community routines, cause, and increase panic and fear of numerous human communities.
- They contaminate and turn inoperable national key facilities, therefore blocking the economic and social life for indefinite periods of time.
- They destroy the trust of human communities in their authorities' capacity to protect the society and the environment, so afflicting the society resilience (Ackerman et al, 2006, pp. 12-14).

The past century knew a remarkable progress in development of biotechnologies and biochemistry, which hugely increased the possibilities to produce and develop biological weapons. Genetic engineering significantly contributed to increase the biological agents' own destructive potential. Industrial production of aggressive agents surged easily and diverse, benefits technological support for increasing the destructive effect, and significantly extended the countries' capability to develop biological agents presenting high risks in case of utilisation in combat (or accidental release) (Miller, pp. 11-13).

As a result, during the latest decades, biological weapons have become a significant concern of responsible officials in national security. The technological revolution of the 90s extended the proliferation of biological weapons among countries, leading to non-state actor participation. Among potential non-state actors, there are terrorist groupings with large financial strength. Therefore, the illegal intentions and activities regarding the use of biological weapon destructive capacity continued to be of current interest and saw an increase in development efforts (Bogdan, Ibid).

CONCLUSIONS

The Convention on biological weapons is a document extremely necessary to the humankind. We insist upon the priority that the value of the Convention should increase a lot in the future, by identification of desirable ways to verify the implementation and respect of its stipulations, therefore, by effective measures of implementing the Convention in international relations. Currently, a swift information exchange is needed to become operational for trustful data regarding the main governmental institution stockpiles that pose adequate biological potential. In view of avoiding dangerous biological situations, research intentions (offensive or defensive) should be known, as well as the typology of utilised agents, the size of projects, quantities of agents used in various activities, and implemented biosecurity measures. Dangerous stem stocks are not to be taken out from storage and transported outside bio-secured facilities. Dangerous stems should be stored only in secure biological research spaces or destroyed in full biosecurity conditions. The priority in the effort of biological prevention includes the participation of all nations in the world (Mackby, pp. 9-12).

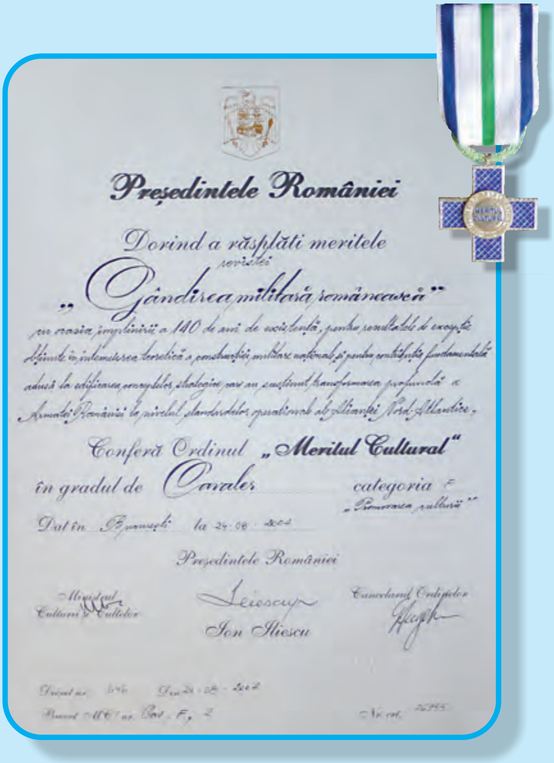
The 1972 Convention should not be regarded as a panacea regarding the problem of biological threat in the world. The increase in measures and capabilities of surveillance, detection, diagnosis, vaccine production, and treatment procedures will amplify the possibilities of diminishing biological threats. Systematic overlapping efforts are necessary, and the international organisations should militate for extending the contents of international agreements established in this domain. It is also necessary to put in practice the common vision of balance and action for increasing the trust and stability in the world.

It is already well known that, in globalisation conditions, the biological crisis should be approached in synchronisation across the globe. Such global conception fosters the coordination of efforts by all nations worldwide, as well as the unitary distribution of recent information, access to critical technologies, joint use of viable treatment procedures, and cooperation among relevant institutions. At national level, a unitary strategic leadership is of paramount importance for biological crisis management, with adequate various measures for prevention, crisis effort, and damage control.

Therefore, concerted efforts are necessary by all nations of the world for generating a new convention in the future, an agreement meant to take over all conclusions and lessons learned from the Covid 19 pandemic, and more effectively support: biological disarmament measures; destruction of dangerous stockpiles; redefining the biosecurity norms; an established presumption of nations' right to protection against offensive biological actions; prevention; monitoring; facility and experiment facility control; as well as mutual support during biological crises. All these should generate protection to the world against biological factors, for securing life on Earth and the progress of tomorrow's society.

BIBLIOGRAPHY:

1. Ackerman, G.A., Moran, K.S. (2006). *Bioterrorism and Threat Assessment*. No. 22. The Weapons of Mass Destruction Commission, Stockholm.
2. Bogdan, V. (2016). Bioterorismul. București: Editura Centrului Tehnic-Editorial al Armatei.
3. Gould, C., Folb, P. *Project Coast: Apartheid's Chemical and Biological Warfare Programme*. United Nations Institute for Disarmament Research. Geneva.
4. Mackby, J. (2003). *Strategic Study on Bioterrorism*. Paris: Center for Strategic and International Studies.
5. Păun, L. (2003). *Bioterorismul și armele biologice*. Editura Amaltea.
6. Milton, L. (2005). *Assessing the Biological Weapons and Bioterrorism Threat*. Strategic Studies Institute. US Army War College. Carlisle.
7. Miller, R. (2005). *The Impact of Quarantine on Military Operations*. USAF Counterproliferation Center. Counterproliferation Paper, no. 31, Alabama.
8. Riedel, S. (2004). *Biological Warfare and Bioterrorism: A Historical Review*. Baylor University Medical Center Proceedings. Vol. 17. No. 4.
9. US General Accountability Office, *Biological Weapons: Effort to Reduce Former Soviet Threat Offers Benefits*, Poses New Risks. (2000). GAO/ NSIAD-00-138, Washington DC.



Preşedintele României

Dorind a răsplăti meritele

revistei

„Gândirea militară românească"

cu ocazia împlinirii a 140 de ani de existenţă, pentru rezultatele de excepţie obţinute în întemeierea teoretică a construcţiei militare naţionale şi pentru contribuţia fundamentală adusă la edificarea conceptelor strategice care au susţinut transformarea profundă a Armatei României la nivelul standardelor operaţionale ale Alianţei Nord-Atlantice,

Conferă Ordinul „Meritul Cultural"

în gradul de Cavaler categoria F „Promovarea culturii"

Dat în Bucureşti la 24.08.2004

Preşedintele României

Ministrul Culturii şi Cultelor

Iliescu
Ion Iliescu

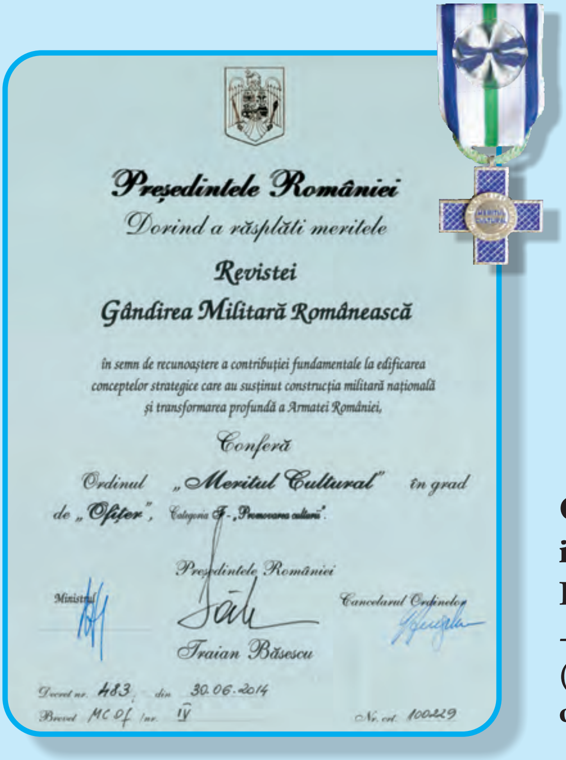
Cancelarul Ordinelor

Decret nr. 646 Din 24.08.2004

Brevet MC/nr. Cav. F, 2

Nr. crt. 26955

Order *"Meritul Cultural"*
in the rank of *"Knight"*,
F Category
– *"Promotion of Culture"*
(Presidential Decree no. 646
on 24.08.2004)



Preşedintele României

Dorind a răsplăti meritele

Revistei

Gândirea Militară Românească

în semn de recunoaştere a contribuţiei fundamentale la edificarea conceptelor strategice care au susţinut construcţia militară naţională şi transformarea profundă a Armatei României,

Conferă

Ordinul „Meritul Cultural" în grad de „Ofiţer", Categoria F - „Promovarea culturii".

Preşedintele României

Ministrul

Traian Băsescu

Cancelarul Ordinelor

Decret nr. 483 din 30.06.2014

Brevet MC Of /nr. IV

Nr. crt. 100229

Order *"Meritul Cultural"*
in the rank of *"Officer"*,
F Category
– *"Promotion of Culture"*
(Presidential Decree no. 483
on 30.06.2014)

gmr.mapn.ro
facebook.com/gmr.mapn.ro